

IFW

PTO/SB/21 (09-04)

Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TRANSMITTAL
FORM**

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

102

Application Number

10/820,111

Filing Date

April 8, 2004

First Named Inventor

Denis Armand Proulx, et al.

Art Unit

8431

Examiner Name

Unknown

Attorney Docket Number

ALC 3125

ENCLOSURES (Check all that apply)☐

Fee Transmittal Form

☐

Fee Attached

☐

Amendment/Reply

☐

After Final

☐

Affidavits/declaration(s)

☐

Extension of Time Request

☐

Express Abandonment Request

☐

Information Disclosure Statement

☒

Certified Copy of Priority Document(s)

☐Reply to Missing Parts/
Incomplete Application☐Reply to Missing Parts
under 37 CFR 1.52 or 1.53☐

Drawing(s)

☐

Licensing-related Papers

☐

Petition

☐Petition to Convert to a
Provisional Application☐Power of Attorney, Revocation
Change of Correspondence Address☐

Terminal Disclaimer

☐

Request for Refund

☐

CD, Number of CD(s) _____

☐ Landscape Table on CD☐

After Allowance Communication to TC

☐Appeal Communication to Board
of Appeals and Interferences☐Appeal Communication to TC
(Appeal Notice, Brief, Reply Brief)☐

Proprietary Information

☐

Status Letter

☐Other Enclosure(s) (please identify
below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name

Kramer & Amado, P.C.

Signature

Printed name

Terry W. Kramer

Date

November 22, 2006

Reg. No.

41,541

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature

Typed or printed name

Moira Anderson

Date

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

BEST AVAILABLE COPY



PATENT

IN THE UNITED STATE PATENT AND TRADEMARK OFFICE

| | | |
|-----------------------|---|--|
| In re application of: | : | Denis Armand Proulx, et al. |
| | : | |
| For: | : | CENTRALIZED INTERNET PROTOCOL/MULTI-PROTOCOL LABEL SWITCHING CONNECTIVITY VERIFICATION IN A COMMUNICATIONS NETWORK MANAGEMENT CONTEXT |
| | : | |
| Serial No. | : | 10/820,111 |
| | : | |
| Filed | : | April 8, 2004 |
| | : | |
| Art Unit | : | 2825 |
| | : | |
| Examiner | : | Unknown |
| | : | |
| Attorney Docket No. | : | ALC 3125 |
| | : | |
| Confirmation No. | : | 8431 |

TRANSMITTAL OF CERTIFIED COPY OF PRIORITY DOCUMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

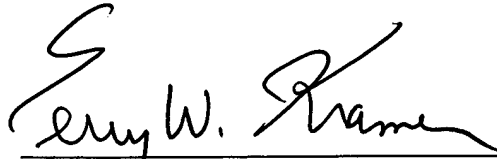
Dear Sir:

Applicants have claimed priority of Application No. 2,425,442 filed April 15, 2003 in Canada, under 35 U.S.C. § 119. In support of this claim, a certified copy of said application is submitted herewith.

Application No.: 10/820,111
Attorney Docket No.: ALC 3125

No fee is believed to be due for this submission. Should any fees be required, please charge our Deposit Account No. 50-0578 and/or please credit any excess fees to such Deposit Account.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Terry W. Kramer". The signature is fluid and cursive, with a large initial "T" and "K".

Terry W. Kramer
Reg. No. 41,541

DATE: November 22, 2006

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, Virginia 22314
Tel. (703) 519-9801
Fax. (703) 519-9802



Office de la propriété
intellectuelle
du Canada

Un organisme
d'Industrie Canada

Canadian
Intellectual Property
Office

An Agency of
Industry Canada

*Bureau canadien
des brevets
Certification*

*Canadian Patent
Office
Certification*

La présente atteste que les documents
ci-joints, dont la liste figure ci-dessous,
sont des copies authentiques des docu-
ments déposés au Bureau des brevets.

This is to certify that the documents
attached hereto and identified below are
true copies of the documents on file in
the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No:
2,425,442, on April 15, 2003, by **ALCATEL CANADA INC.**, assignee of Denis A.
Proulx, Craig Ellert Timmerman, Felix Katz, Margaret Rachniowski, Afshan Zabihi and
Macmohana S. Viridy, for "Connectivity Verification for Internet Protocol/Multi-Protocol
Label Switching Data Communications Networks".

L. Régimbald

Agent certificateur / Certifying Officer

April 14, 2004

Date

Canada

(CIPO 68)
04-09-02

OPIC  CIPO

Abstract

A framework for connectivity verification is provided. The framework includes a connectivity verification server performing unattended connectivity verification, and a connectivity verification application, both the connectivity verification server and connectivity verification application operating in a network management context. Connectivity verification jobs are defined via the connectivity verification application and the connectivity verification server is configured accordingly. Connectivity verification jobs can also be scheduled. The connectivity verification application also provides a display of connectivity verification results. The results of each connectivity verification job may be compared against a desired connectivity profile and deviations from the connectivity profile may be used to raise alarms. Connectivity verification results, including alarm information, are further used to generate a network map displaying selected connectivity verification results. The advantages are derived from using the framework to perform unattended scheduled connectivity verification at reduced operational costs.

**Connectivity Verification for
Internet Protocol / Multi-Protocol Label Switching
Data Communications Networks**

Field of the invention

[01] The invention relates to data network management, and in particular to methods and apparatus for centralized connectivity verification ensuring adherence to service level agreements.

Background of the invention

[02] In the field of Internet Protocol (IP) / MultiProtocol Label Switching (MPLS) data communications, it is known to verify whether two data network nodes can reach each other by employing functionality provided by a "ping" and a "traceroute" command. The implementation of the ping and traceroute command functionality specification is described in RFC-1147 which is incorporated herein by reference. A short summary of the relevant concepts of the ping and traceroute commands follows:

[03] Persons of ordinary skill in the art would understand that data communications networks conveying data packets in accordance with the IP protocol and the MPLS protocol do so in accordance with a store and forward discipline. At each data network node in a communications network, a packet is received via an input port, stored, an output port determined in real-time, and the packet is forwarded over the determined output port. Real-time port determination is known as routing functionality and is performed by a router network element. The real-time determination of the output port is made dependent on a variety of factors including: destination addressing information held in packet headers, forwarding class associativity, packet traffic

differentiation, operational states of inter-connecting links between network nodes, transport bandwidth availability, etc.

[04] Persons of ordinary skill in the art would understand that data communications networks conveying data packets in accordance with the IP protocol, do so in accordance with a best-effort packet transport discipline. The best-effort discipline does not guarantee that data packets will reach their destinations, does not guarantee bounded packet arrival latencies, does not guarantee bounded packet arrival jitter, etc. In fact packets specifying the same source network address and the same destination network address do not necessarily follow the same transport path in a data communications network, which is known in the art as loose source routing.

[05] The real-time output port determination described above may lead to situations in which packet transport loops are established. Each IP packet carries a Time-To-Live (TTL) specification in its header, which is an integer header field value which is set by a source data network node sending the packet (or a gateway at an edge between a customer network and a service provider network) and decremented at each data transport node forwarding the packet. When the TTL value reaches zero (0), the packet is discarded.

[06] Although simple, this approach puts a lot of pressure on IP network design to ensure that only a small number of data transport nodes, and therefore interconnecting links, are traversed between a source data network node and a destination data network node. The physical implementation of the interconnecting links is varied and may include additional data/packet transport protocols, therefore from the point of view of connectivity verification, the data communications network infrastructure between two data transport nodes is referred to as a "hop" to make an abstraction thereof.

[07] As mentioned herein above, the best-effort packet transport discipline does not guarantee bounded packet arrival latencies. Latency is the amount of time it takes for a packet to traverse a communications network from its source

data network node to its destination data network node. Latency is typically measured in milliseconds and includes physical data transport delays associated with physically conveyance of packets over physical interconnecting links, as well as packet processing delays incurred by packet while being stored at transport network nodes, in a transport path between the source network node and the destination network node, while pending determination of output ports.

[08] As mentioned herein above, the best-effort packet transport discipline does not guarantee bounded packet arrival jitter. Jitter is a measure of the variation of packet inter-arrival delays, and relates to a measure of the standard deviation of a group of delays incurred by a group of individual data packets typically associated with a data stream used in provisioning a data service.

[09] The provision of data services, which is beyond the present description, is dependent on the resultant Quality-of-Service provided. Quality-of-Service is a combination of bandwidth, arrival delay, and jitter specifications for a particular data service provisioned end-to-end over a given interconnecting communications network infrastructure.

[10] A person skilled in the art would understand that the MPLS transport protocol has been developed in order to provide high Quality-of-Service packet transport. Although, delays associated with physical propagation packets over physical interconnecting links can only be reduced to a certain extent, the MPLS technology provides: bandwidth reservation on the interconnecting links to ensure a resource availability, strict (pre-specified) routing / transport path to minimized packet processing delays along the path, and consolidated multi-transport layer switching minimizing switching delays at switching network nodes in the path. Packets having the same source network address and the same destination network address may follow different transport paths dependent on a Service Level Agreement (SLA) specification for each packet.

[11] It is the adherence to a service level agreement in an MPLS environment, and the need to adhere to a service level agreement specification in a best-effort IP environment that is being addressed in the present description.

[12] Implementation of ping and traceroute functionalities includes the return conveyance of at least one individual echo return Internet Control Message Protocol (ICMP) packet in a data communication network between a source network node and a destination network node to verify connectivity between remote computers.

[13] The extent to which connectivity is verified by ping packets, as they are known, relates to reachability, see Fig. 2. Ping packets carry a TTL value, and therefore reachability includes: an assessment as to whether there is at least a sequence of interconnecting links which when traversed a packet can be conveyed between the source network node and the destination network node, as well an assessment as to whether a bound sequence of interconnecting links exists. It is emphasized that each packet tests connectivity between a pair of pre-specified source network node and destination network node.

[14] Besides reachability, each ping packet is also stamped with a time value corresponding to the time at which the ping packet was sent from the source network node. Upon the return of the ping packet at the source network node, the aggregate return transport delay is calculated. In sending a group of ping packets, the corresponding group of aggregate return transport delays are used to determine: minimum delay, maximum delay, average delay (in milliseconds), and jitter. The determined minimum delay, maximum delay, average delay, and jitter is referred to as packet transport statistics.

[15] The extent to which traceroute packets verify connectivity, as they are known, relates network node discovery between a source to a destination network node, see Fig. 3. Implementing traceroute functionality employs groups of ICMP echo return packets bearing increasing TTL values, and directed to the destination network node. Traceroute packets are returned to

the source network node when the TTL value is decremented to zero, determining a transport network node incrementally further along between the source network node and the destination node.

[16] For a source routed Label Switched Path (LSP) pre-established path, physical network nodes incrementally further along the LSP transport path may not return traceroute packets as the traceroute packet is encapsulated while in transport through the LSP with the TTL value only being decremented at the distal end of the LSP which does return a traceroute package, see Fig. 4. Traceroute packets are returned by network nodes beyond the distal end of the LSP.

[17] In a best-effort IP environment, it cannot be guaranteed that all traceroute packets are routed the same as packet processing conditions change dynamically at network nodes between the source and the destination network nodes. A degree of stability in a communications network is expected, although not guaranteed, which when traceroute packet are sent in a relatively rapid succession, results in the group of traceroute packets following substantially the same transport path.

[18] A returned traceroute packet is used to extract transport delay information. Statistical information is derived from successive sequences of traceroute packets. Therefore transport delay and jitter profiles can be provided for each transport path between a pair of network nodes in a data communications network. The extent to which these delay and jitter profiles can be used to derive per-hop statistics is left to higher level applications interpreting the statistical information which are beyond the scope of the present description.

[19] Having provided an overview of ping and traceroute functionality, it is important to emphasize that, ping and traceroute packets are sent from a source network node and returned to the same source network node. The resulting statistics are also made available by and at the source network node.

[20] Service providers include organizations and data communications network infrastructure providing data transport services to customers. Services include best-effort data transport, MPLS data transport, as well as differentiated services such as Virtual Local Area Networking (VLAN) in support of Virtual Private Network (VPN) connectivity.

[21] Currently service providers make extensive use of ping and traceroute functionality to verify connectivity on a very limited basis. Typically an operator needs to physically and manually log-in on each remote source network node to access a Command Line Interface (CLI), issue necessary ping and/or traceroute commands from a prompt specifying network node addressing manually, capture the output of the console, and retrieve the output from the remote source network node.

[22] In service provider communications network it is more important to verify connectivity between individual routers. Referring to Fig. 1, five fully meshed routers R1, R2, R3, R4 and R5 providing VPN services VPN1 and VPN2 are shown. Connectivity verification between Location 1 and Location 3 can be performed manually in two steps: ping/traceroute test T1 is run from R1 towards R3 and a second ping/traceroute test T2 is run from R3 towards R1. Each time a ping/traceroute test is run, the operator has to log-in on the source router, run the ping/traceroute test, and retrieve the results.

[23] If connectivity verification is required between all peer routers in VPN1 more test steps would be required, for example ping/traceroute test T3 verifies connectivity from Location 2 to Location 3, and another ping/traceroute test would be necessary to verify connectivity to Location 3 from Location 2. Also, another two ping/traceroute tests would have to be done between Location 1 and Location 2.

[24] The operator has to perform more ping/traceroute tests for the other VPNs, for example VPN2 between Location 2 and Location 4.

[25] The connectivity verification has to be done in two separate steps between each pair of locations, and it is not obvious to the operator which router IP address and VLAN IDentifier (VPN1/VPN2) to use from which router. This level of operator involvement is inadequate as command entry is a very time consuming, complex, and error prone procedure leading to large operational overheads incurred by service providers. In particular, manual command entry makes it impossible for connectivity verification to be performed in an environment in which a large number of customers are serviced by a service provider using an infrastructure of a large number of communications network nodes interconnected via a large number of links. Meaningful statistics need be derived from a large number of ping/traceroute tests.

[26] Persons of skill in the art understand that packet traffic patterns vary over a period of time and are typically cyclical over the time of a day and cyclical over a week. It is important to both customers and service providers that connectivity verification be performed during peak hours (business hours and evenings) and peek weekdays (workdays and weekends). Therefore it is apparent that if manually directed connectivity verification is time consuming, then manual connectivity verification within a test window would be impossible due to overwhelming operational overheads involved. The number of connectivity verification tests grows with the number of location combinations for each VPNs making connectivity verification even more complex and time consuming.

[27] The closest prior art relates to network topology discovery and includes:

[28] A prior art United States Patent 6,502,130 B1 entitled "System and Method for Collecting Connectivity Data of an Area Network" which issued on December 31st, 2002 to Keeler, Jr. et al. describes a system and method which collects dynamic connectivity data from an area network interconnecting multiple computing devices. The dynamic connectivity information is combine

in a data warehouse with static network information, relating to the various users and their privileges. The combined data stored in a data warehouse permits the identification of each user and the various privileges of the user, correlated to its connection port. The productivity data is collected using commands in the simple network management protocol (SNMP). SNMP commands query all network devices such as hubs, routers, and gateways to other networks to obtain port connectivity information such as the identity of the ports being used by each network user. Although inventive, the solution proposed by Keeler Jr. et al. only achieves Open Systems Interconnect (OSI) Layer 2 and 1 connectivity discovery in support of billing applications for users subscribing to roaming network access services. Keeler Jr. et al. do not address issues related to ensuring adherence to service level agreements in real-time.

[29] A prior art United States Patent 6,205,122 B1 entitled "Automatic Network Topology Analysis" which issued on March 20th, 2001 to Sharon et al. describes a system and method for automatic detection of physical network topology, by correlating information from computers connected to a network. Although inventive, the solution presented by Sharon et al. does not address issues related to ensuring adherence to service level agreements in real-time.

[30] A prior art United States Patent 6,397,248 B1 entitled "System and Method to Discover End Node Physical Connectivity to Networking Devices" which issued on May 28th, 2002 to Iyer describes an apparatus and method for determining physical connectivity between end nodes and networking devices within a network. Iyer addresses issues related to the SNMP protocol's inability to ascertain the physical connection between end nodes and networking devices. Although inventive, the solution presented by Iyer does not address issues related to ensuring adherence to service level agreements in real-time.

[31] A prior art United States Patent 6,405,248 B1 entitled "Method and Apparatus for Determining Accurate Topology Features of a Network" which issued on June 11th, 2002 to Wood describes a method for determining accurate

topology features of a given network utilizing source address tables. The solution proposes acquiring source address table information from each port of each network switching node at regular intervals to determine when a particular source address was learned and when discarded. The source address information is used to issue Address Resolution Protocol (ARP) queries to ensure that the source address information is valid. While inventive, the solution presented by Wood does not address issues related to ensuring adherence to service level agreements in real-time.

[32] A prior art United States Patent 5,974,237 entitled "Communications Network Monitoring" which issued on October 26th, 1999 to Shurumer et al. describes a proprietary method for monitoring a communications network comprising a plurality of node equipment such as switches, and link equipment such as fiber optic links in which proprietary performance parameters of individual vendor specific components of the node equipment are used to determine an overall proprietary performance parameter for the node equipment. By comparing like proprietary performance parameters for individual network elements, the performance of different types of proprietary network elements can be compared with each other. Parameters which can be monitored include quality of service, cell discard, cell loss, and other measures of network performance. Connection tracing through the plurality of node equipment and link equipment is used employing proprietary means to provide topology discovery. While inventive, the solution presented by Shurumer et al. does not address issues related to ensuring adherence to service level agreements in real-time.

[33] Other developments include, a prior art United States Patent 6,222,827 B1 entitled "Telecommunications Network Management System" which issued on April 24th, 2001 to Grant et al. describes a system for managing a Synchronous Digital Hierarchy (SDH) network and proposes the tracking and processing of network related data in support of specifying connectivity parameters for establishing data pipes. The solution relates to a network management system

which forms an overall view of the network and its condition from which the system gives configuration commands to each transmission equipment so that all configuration changes can be performed significantly more rapidly. While inventive, the solution presented by Grant et al. does not address issues related to ensuring adherence to service level agreements in real-time.

[34] Reducing operating expenditures is important service providers. Addressing these concerns is especially important in large and complex Service Provider IP/MPLS networks. There therefore is a need to solve the above mentioned issues.

Summary of the invention

[35] In accordance with an aspect of the invention, a framework for connectivity verification is provided. The framework includes a connectivity verification server performing unattended connectivity verification, and a connectivity verification application, both the connectivity verification server and connectivity verification application operating in a network management context.

[36] In accordance with another aspect of the invention, connectivity verification jobs are defined via the connectivity verification application and the connectivity verification server is configured accordingly.

[37] In accordance with a further aspect of the invention, connectivity verification jobs are scheduled and the connectivity verification server performs scheduled connectivity verification.

[38] In accordance with a further aspect of the invention, the connectivity verification application also provides a display of connectivity verification results.

[39] In accordance with a further aspect of the invention, the results of each connectivity verification job may be compared against a desired connectivity profile and deviations from the connectivity profile may be used to raise alarms.

[40] In accordance with yet another aspect of the invention, connectivity verification results, including alarm information, are further used to generate a network map displaying selected connectivity verification results.

[41] The advantages are derived from using the framework to perform unattended scheduled connectivity verification at reduced operational costs.

Brief description of the drawings

[42] The features and advantages of the invention will become more apparent from the following detailed description of the preferred embodiment(s) with reference to the attached diagrams wherein:

FIG. 1 is a schematic diagram showing prior art manual connectivity verification;

FIG. 2 is a schematic diagram showing a ping connectivity verification test being performed between a source and destination node;

FIG. 3 is a schematic diagram showing a traceroute connectivity verification test being performed between a source and destination node;

FIG. 4 is a schematic diagram showing a traceroute connectivity verification test being performed between a source and a destination node via an LSP;

FIG. 5 is a schematic diagram showing elements of a connectivity verification framework in accordance with an exemplary embodiment of the invention;

FIG. 6 is a schematic diagram showing network nodes participating in a VPN and a fully meshed bi-directional group of connectivity validation tests to be performed in accordance with the exemplary embodiment of the invention; and

FIG. 7 is a schematic diagram showing connectivity verification performed in accordance with the exemplary embodiment of the invention.

[43] It will be noted that in the attached diagrams like features bear similar labels.

Detailed description of the embodiments

[44] Fig. 5 shows a framework in accordance with an exemplary embodiment of the invention. A connectivity verification application makes use of an IP map application and/or a Layer 2 map application to select source and destination network nodes from a selection of network node tracked via a containment hierarchy by a network management server.

[45] The selected source and destination network nodes are used to define a connectivity verification job. A schedule may be defined for the connectivity verification job. The definition of the connectivity verification job includes specifying connectivity verification parameters including the number of connectivity verification tests to be performed and thresholds to be applied to connectivity verification results returned.

[46] In accordance with another implementation of the exemplary embodiment of the invention, by specifying a source and destination network node pair, a pair of bi-directional connectivity verification tests is defined.

[47] In accordance with another implementation of the exemplary embodiment of the invention, IP and Layer 3 objects having a source and destination network node may be selected from the containment hierarchy.

Such objects include IP links, LSPs, etc. VPNs may specify a large group of participating network nodes. In accordance with another implementation of the exemplary embodiment of the invention, by specifying a group of network nodes fully meshed bi-directional connectivity verification tests will be performed between the group of network nodes. See Fig. 6 for a selected group of five network nodes and the bi-directional connectivity verification tests to be performed therebetween although fully meshed interconnecting links may not exist therebetween.

[48] Each connectivity verification job can be dispatched for immediate execution via a connectivity verification server or stored with the connectivity verification server for delayed and/or repeated execution.

[49] The connectivity verification server queues connectivity jobs with a Command Line Interface Processor (CLIP) at the appropriate time specified by the scheduling information (or immediately upon request). The CLIP processor takes over the issuing of commands to source destination nodes and the retrieval of connectivity verification results in an interaction session in which the CLIP processor logs-on the source network node. The CLIP processor sequences command issuance so as not to over burden the communications network with ICMP traffic.

[50] Connectivity verification results are provided to the connectivity server which compares the connectivity verification results against thresholds specified for the connectivity verification job to ensure adherence to SLA agreements. When thresholds are reached alarms are raised with an alarm server. The alarm information may also be propagated to the connectivity verification application. The alarm information provided to the connectivity verification application may be subsequently updated by the alarm server.

[51] In accordance with another implementation of the exemplary embodiment of the invention, each connectivity verification result is compared

against a threshold profile comprising at least two thresholds, multiple thresholds being used to implement multiple levels of alarm severity.

[52] Connectivity verification results are also provided to the connectivity verification application. The connectivity verification application uses the connectivity verification results and alarm information to highlight Layer 2 and Layer 3 objects affected by the alarm information. The connectivity verification information may be interacted with to cause the display of Layer 2 and Layer 3 objects associated with a particular connectivity verification test and/or connectivity verification job.

[53] In accordance with the exemplary embodiment of the invention, the problem of verifying IP connectivity in a service provider IP/MPLS network using an NMS system is addressed by:

- Performing directed Ping and Trace Route connectivity test using source and destination objects.
- Performing connectivity test using Routers and IP Interfaces.
- Performing connectivity test using MPLS LSP.
- Performing connectivity test within IPVPN. (VRF – VLAN ID) See RFC 2547 L3VPN incorporated herein by reference.
- Performing connectivity to unmanaged routers (IP address discovered)
- Scheduling the 'N' connectivity test to verify connectivity periodically.
- Scheduling the 'N' connectivity test to summarize statistics for the IP traffic characteristics (Delay, Jitter, loss) of packets.
- Ability to configure alarm threshold on the 'N' connectivity test schedule results to ensure service level agreements (SLA) are met.
- Highlighting the single or many routes of the packet that failed or succeeded on the NMS IP MAP

[54] According to the present invention, the NMS provides a network view of the IP objects including Routers, IP links, IP interfaces, IP address of

Unmanaged Routers, LSP and VPN, making the connectivity verification test easier to create.

[55] The operator is provided with means to collect the statistics from 'N' connectivity verification tests.

[56] The operator can easily run a connectivity verification test via a single click to verify VPN connectivity.

[57] A mechanism is provided to schedule 'N' connectivity verification tests and to collect the results in a central location for analyzing the data.

[58] Immediate alarms generated from the results of 'N' connectivity verification tests in view of thresholds are provided.

[59] Referring to Fig. 7, according to a use scenario of the exemplary embodiment of the present invention, the NMS operator can easily create one schedule to test the VPN connectivity shown.

[60] In the example only two VPN exist. The operator creates one schedule and identifies the connectivity verification tests (T1,T2,T3,T4,T5,T6,T7,T8).

[61] The NMS operator with a single click initiates the connectivity verification tests.

[62] The NMS operator can specify that the connectivity verification test be executed periodically.

[63] The NMS operator can set thresholds for expected connectivity verification results to trigger alarms when IP packets flow requirements are not met to ensure adherence to SLA agreements.

[64] The NMS CLIP processor sends Ping and Trace Route commands (operations) to the routers. The connectivity verification tests can specify one or more of the following NMS objects as the source for the operation:

- Router (Router managed by the NMS),
- First Hop LSP (determines the Router), and
- VPN (VRF name).

The NMS destination objects include:

- Any IP address (NMS managed Router and Unmanaged Router),
- Router,
- Router Interface (Numbered and Unnumbered (Router ID - string)), and
- LSP (the destination router will be determined by the destination endpoint of the LSP).

[65] The operator can configure specific connectivity verification parameters for the connectivity verification test such as the number of pings to execute, packet size, data fill patterns, time to wait for response, type of service.

[66] The operator can set threshold on the packet statistics for X number of connectivity failures, round trip delay, jitter, packet drop requirements.

[67] The NMS is then able to perform one of the following tasks for the entries specified:

1. Ping operation from the source to the destination (results and statistics displayed to the operator).
2. Traceroute operation from the source to the destination (results and statistics displayed to the operator).
3. Highlight the results of the traceroute operation. This will highlight layer 2 and layer 3 objects on the NMS Layer 2 and IP maps.
4. Save the results as text or CSV format to a local file to be analyzed later.
5. Historical results from all operations are available in a result log on the connectivity verification server.
6. Highlight objects based on what is selected in the operation list or the result list.
7. Export and/or import the Operation List.

8. For the scheduled connectivity verification test, summarize the packet statistics for historical review.
9. For the scheduled connectivity verification test, generate alarms when the thresholds are met/exceeded.

[68] The following is a more detailed description of features of the invention as exemplarily implemented in an exemplary connectivity verification application in accordance with the exemplary embodiment of the invention. Heretofore the connectivity verification application and the subject matter of the invention is referred to as an "IP Maintenance and Diagnostics" solution. Any limitations mentioned in the following description relate to the particular implementation described and should not be interpreted as limiting the invention described herein in any way.

GLOSSARY

| | |
|--------------|---|
| CLI | <i>Command Line Interface.</i> This is a command driven text based user interface to a device. |
| CORBA | <i>Common Object Request Broker Architecture.</i> An architecture that enables communication between program objects regardless of the programming language the objects are written in or the operating system they run on. |
| CSV | <i>Comma Separated Value.</i> A way of recording values in text format with each value followed by a comma. |
| VPN | <i>Virtual Private Network.</i> |
| VRF | <i>VPN Routing and Forwarding.</i> |

INTRODUCTION

This Feature Specification outlines expected IP Maintenance and Diagnostics functionality. It allows users of the Alcatel NMS Network Manager to gather information about the IP connectivity in the network for maintenance and diagnostics purposes.

Terminology

Frequency – The time between each iteration of a schedule.

VPN – This document, unless otherwise specified, deals with routed IP VPNs.

As such, the term indicates a set of IP-enabled systems and networks that communicate over a shared infrastructure with comparable access and security practices to a private network.

Iteration – One run of a schedule (i.e. one summary period).

Schedule - A schedule is a list of ping operations that will be executed at a specific time.

FUNCTIONAL OVERVIEW

Summary of Functionality

The IP Maintenance and Diagnostics provides the following main functions:

- Fn1: Performing Ping Operations.
- Fn2: Performing Traceroute Operations.
- Fn4: Queuing Ping and Traceroute Operations.
- Fn5: Determine statistics from each Operation (such as jitter).
- Fn6: Viewing the results of Ping and Traceroute Operations.
- Fn7: Saving results from Operations to a user defined file in different formats.
- Fn8: Highlight affected objects from a Ping or Traceroute.
- Fn9: Saving and Opening Operations Lists.
- Fn10: Scheduled Ping Operations
- Fn11: Configurable Threshold Values
- Fn12: Create an alarm when a threshold is exceeded for a Schedule
- Fn13: Summarized statistics

IP Maintenance and Diagnostics will also support the following key functionality:

- NFn1: Scheduled Traceroute Operations.
- NFn2: Configurable Traceroute and Ping ICMP parameters.
- NFn3: Ping and Traceroute from source NMS
- NFn4: Partitioned Nodes as Ping and Traceroute source objects
- NFn5: SNMP support for MIB 2925

Typical Application

IP Maintenance and Diagnostics allows users access to information that will help them with maintenance and diagnostic issues associated to their IP network.

i. Ping and Traceroute

Ping and Traceroute commands are executed on a router so information can be displayed to the user. It gives users the ability to perform traceroute and ping operations to determine connectivity information such as delay, packet loss, jitter and routes.

The IP Maintenance and Diagnostic system consists of a client user interface and a server process. The server process controls the connection to the router and the ping, traceroute and scheduling operations (see Figure 0-1). It is running on the active Alcatel NMS and will be active on the standby if a switchover occurs.

Each IP Maintenance and Diagnostic client connects to the server process on the active NMS to send ping and traceroute operations to the routers. The client can specify one or more of the following objects as the source for the operation:

- Router Management IP Address (Router supported by the 5620)
- Node (with an IP Address)
- Router Interface
- First Hop LSP (the source router will be determined by the source endpoint of the LSP)
- VRF name (with a supported router specified).

The client can specify one of the following as the ping destination:

- Any IP address (whether it is a NMS managed object or not).
- Router ID (Router managed by the 5620)
- Node (by specifying its IP Address)

Pasting in one of the following objects known to the NMS can also specify a destination:

- Router Interface (the destination endpoint will be the router interface IP address, in the case of unnumbered, it is the router ID)
- LSP (the destination router will be determined by the destination endpoint of the LSP)

The client is then able to perform one of the following tasks for that entry (see Figure 0-1):

10. Ping from the source to the destination (results and statistics displayed to the user).
11. Traceroute from the source to the destination (results and statistics displayed to the user).
12. Save the results as text or CSV format to a local file.
13. Historical results from all operations are available in a result log on the server.
14. Highlight objects based on what is selected in the operation list or the result list.
15. Save and/or retrieve the Operation List.

Ping and traceroute operations are very easy to initiate. There can be multiple operations at one time, but to protect against performance issues, only one operation is allowed at any time to one source router. The application has the ability to queue multiple operations that are initiated so the user does not have to wait for one operation to complete before initiating the next. The only visible effect the user will see is that the operation may take a bit longer to complete.

The results from each individual ping and traceroute can be viewed. The information includes statistics such as jitter, percent of packets lost, and delay. After the user has configured ping and traceroute operations, they have the ability to save that list for future use (no operation results are saved). To use a previously saved operation list, they must open the file containing the operations. No validation occurs when a list is retrieved into the application and the last results for those newly retrieved operations are not available.

ii. Scheduled Operations

Scheduled ping operations perform similar to user-initiated operations and have the same limitations.

The Scheduled operations have the added functionality that allows them to store results every time the operations run, and to create summary statistics. It gives the customer the ability to check connectivity between endpoints at specific times and/or specific iterations. This can help determine if SLA's are being met for customers VPN and/or if there is a failure in the network (see Figure 0-2). An example implementation of a schedule for Customer A VPN1 in Figure 0-2 can be seen in Figure 0-8. The user can customize thresholds to raise alarms if any of the summary statistics do not meet defined SLA values.

The functionality defined in section i applies to scheduling, except that the server performs the initiation of the operation at a set time and frequency rather than the user initiating the operation. The Server initiates the operations based on the scheduling information contained for each schedule. If a schedule is running, and a user tries to invoke an operation to the same router, they will be warned and the operation will be queued until the schedule has finished with the specified source router. If a user is currently performing an operation on a router and a schedule runs with the same source defined, the user operation is cancelled and the user is notified. The schedule has priority at all times. All parameters defined for a schedule applies to all the contained operations in that schedule.

The individual results and summary statistics from the operations can be viewed at any time. The summary information includes statistics such as jitter, percent of packets lost, and delay. The individual results show exact error codes, such as node unreachable, and delay values that were used in the calculation of the summary statistics. The results can then be saved to a file for further analysis. The summary statistics, which are calculated based on the individual results per operation, can then be used to raise alarms to the fault management system. The summary results are based on the user specified summary period, which is a number of individual results contained in a summary period.

The user can specify thresholds for each schedule. These thresholds apply to all operations contained in that schedule. If a threshold is exceeded, based on the

summary statistics, an alarm will be generated to the fault management system with the user-specified severity.

FUNCTIONAL DETAILS

Overview

IP Maintenance and Diagnostics consists of 2 clients, a main Operation Window and a Scheduling Window. Both are launched through the NMS main menu, and are not context sensitive (i.e. a router does not have to be selected for the menu to be enabled).

The operation window contains 2 types of operations, ping and traceroute. The ping and traceroute operation each allows parameters to be specified for each individual operation. After an operation has been configured, it is then added to an operation list. It does not automatically start the ping or traceroute operation, it must be initiated by selecting the operation, right clicking, and selecting "initiate" from the popup menu. The operation can be cancelled or deleted by the same popup menu. The operation list can then be saved to a user defined local file. The list can then be retrieved at a later time to allow the user to reuse operations.

After an operation completes, the user selects the completed operation and the results will then appear in the result list. This information includes the delay for each individual ping issued in a ping operation, jitter, maximum delay, average delay, minimum delay, errors, etc. The information in the result list can then be saved to a local file in one of two formats, text or CSV. Historical results are located on the server and contain the results from every ping and traceroute operation that has taken place.

The scheduling window contains ping operations that can be run at a specific time. The operations contained in a schedule run starting at the specified start time, at every frequency (e.g. if the frequency is 10 minutes, all operations in the schedule run every 10 minutes) until it reaches the end time. The user can create an operation directly in a schedule, retrieve operations from a file or they can copy and paste/drag and drop it from another schedule or the operation window. All ping operations contained in a schedule have the same parameters except for the destination and source fields.

The results include individual ping results and summary statistics. The summary statistics are the same as those for a regular ping operation except they are calculated over a summary period (e.g. for every 10 iterations calculate the statistics). For each summary period, the user can view the individual ping values and the time that they were returned from the router. The summary results and individual ping results can be saved to a file in one of two formats, text or CSV.

A schedule can also contain threshold values for Jitter, Delay and Packet Loss. If any of these threshold values are exceeded, an alarm can be generated to the fault management system. The schedule uses the summary statistics from each operation to determine if a threshold has been exceeded. It will then generate an alarm to the fault management system with the user-specified severity. The user will also be able to see in the scheduling window any operations that had an alarm or error generated for that summary period.

IP Maintenance and Diagnostics Operation Window

The IP Maintenance and Diagnostics Operation window contains 3 areas, Operation List section, Results section and the Response Pane. The operation list section contains all the pings and/or traceroutes that have already been created or queued and can be initiated. This allows the user to perform multiple operations at one time. To view the results of an operation, it must be complete, and then selecting it from the operation list will update the result section with the operations results. If the selected operation is in progress, the result window will automatically update when it receives the results.

The result section contains the information from that ping or traceroute including the delay, result and size from each individual ping or traceroute (hop) in the operation. The Response Pane includes statistics on the entire ping operation, such as jitter and packet loss percentage, and it will also be the area that displays any errors that occurred in the operation. In the case of a traceroute operation, the statistics are based on the selected hop in the result list. The Operation List and Result List have scrollbars that appear when the list

grows larger than their viewable area. A splitter window that separates the lists also allows the user to choose how large the viewable area is for each.

The Operation window contains common functionality that is used in the Scheduling window.

iii. Launching IP Maintenance and Diagnostics

Selecting "Administration->IP Diagnostics" from the NMS main menu opens the IP Maintenance and Diagnostics client. Restriction of this command is only done through scope of command for the main menu; there are no other restrictions to opening the window. It can be displayed at any time, a router or node does not have to be selected. If a valid router or node is selected when the window opens, it will by default be the specified source object with the name and IP address already filled in for the source field for an operation dialog. If it is an invalid object, the source fields will be blank and the user will have to specify a valid router or node. The user is allowed to open only one operation window at a time. If the user selects the IP Diagnostics menu a second time, and the window is already launched, it will bring it to the front for the user. The IP Maintenance and Diagnostics scheduling window can also open the operation window with the "File->Operation Window" menu item.

iv. Menus and Toolbars





| Icon | Menu Item | Description |
|---|----------------------------|---|
|  | Operation->New->Traceroute | Open the Traceroute window for creation. |
|  | Operation->Initiate | Initiate the selected operation(s). |
|  | Operation->Cancel | Cancel the selected operation(s). |
| None | Result->List LSP | List the LSPs between the selected source and destination in the Result List. |
|  | File->Schedule Window | Open the Schedule window |

Table 0-1: Menu items and associated Toolbar Icons

Common menu items and toolbars are found in Section xxv. The menu items identified in Table 0-1, are specific to the IP Maintenance and Diagnostics Operation window.

v. Saving the Result List to a Local File

Operation results can be saved to a local file in one of two formats, CSV or TXT.

See section xxvii for a description of the save dialog.

Text Format

Ping Toronto - Ottawa

Source 138.120.15.90: vrf - VPN1 Destination 13.13.13.2

| Seq | Source | Destination | Delay (ms) |
|-----|---------------|-------------|------------------|
| 1 | 138.120.15.90 | 13.13.13.2 | 112 |
| 2 | 138.120.15.90 | 13.13.13.2 | Node Unreachable |
| 3 | 138.120.15.90 | 13.13.13.2 | 98 |

%Loss: 0.0 Jitter (ms): 0.0 min/max/avg (ms): 1.0/1.0/1.0

Traceroute Toronto - Ottawa

Source 138.120.15.90: vrf - VPN1 Destination 56.56.56.56

| Seq | Destination | Delay (ms) |
|-----|-------------|-------------------------|
| 1 | 12.12.12.1 | 10, Node Unreachable, 5 |
| 2 | 13.13.13.2 | 4, 6, 6 |

Figure 0-1: Text Format Example (Ping and Traceroute)

When the user selects the text format for saving results ("Save as Type" field), it will save it in a standard space formatted file. The text file will also contain the statistics associated with the operation(s) appended to the end of the file (see Figure 0-1).

CSV Format

Ping, Toronto - Ottawa

Source, 138.120.15.90: vrf - VPN1, Destination, 13.13.13.2

Seq, Source, Destination, Delay (ms)

1, 138.120.15.90, 13.13.13.2, 112
 2, 138.120.15.90, 13.13.13.2, Node Unreachable
 3, 138.120.15.90, 13.13.13.2, 98

%Loss (ms), 0.0

Jitter (ms), 0.0

Min (ms),1.0

Max (ms),1.0

Avg (ms),1.0

Traceroute, Toronto - Ottawa

Source,138.120.15.90: vrf - VPN1, Destination, 13.13.13.2

Seq, Destination, Delay (ms)

1,12.12.12.1,10,Node Unreachable,5

2,13.13.13.2,4,6,6

Figure 0-2: CSV Format Example (Ping and Traceroute)

When the user selects the CSV format for saving results ("Save as Type" field), it will save it in a comma separated formatted file. The text file will also contain the statistics associated with the operation(s) appended to the end of the file (see Figure 0-2).

vi. Operation List

| Column | Description |
|----------------|--|
| Type | The type of operation, Ping or Traceroute (see Table 0-3). |
| Name | The Name associated to the operation |
| Source | The router the operation is being performed on |
| Destination | The object the operation is being performed to |
| Timeout (ms) | The timeout to wait for a response from the destination. |
| Quantity | The number of individual pings in this operation |
| Interval (sec) | The interval between sending each ICMP packet. |
| Status | The status of the operation (see Table 0-5 for a list of status values). |

Table 0-2: Parameters displayed in the operation list for each operation

The operation list contains the ping and traceroute operations specified by the user. The operations appear in the order they are added.



| Icon | Description |
|---|----------------------|
|  | Ping Operation |
|  | Traceroute Operation |

Table 0-3: Icon representation of the "Type" field in the Operation List

The list will contain all the defined ping and traceroute operations created by the user and they are distinguishable by the "Type" column (see Table 0-3). IP Maintenance and Diagnostics does not allow concurrent operations to the same router. If multiple operations are queued for the same router, the status of the waiting operation(s) will be "In Progress" while the currently running/queued operations complete. If the user attempts to close the application with operations still "In Progress", a warning will appear to the user. If the user chooses to continue with the close of the application, the operations will be cancelled to the server before closing.

| Item | Description |
|-----------------|--|
| Initiate | Initiate the operation(s) on the node. This menu option is only enabled if an operation is currently not in progress |
| Cancel | Cancel the operation(s) once it has been initiated. This menu is only enabled if an operation is currently in progress |
| Delete | Delete the operation(s) from the list |
| Save Operations | Save the operation list for future use |
| Highlight | Highlight all known objects associated with the operation (see section xxxi) |

Table 0-4: Menu items for the operation list popup menu

Double clicking on an operation in the operation list will open the appropriate operation window to allow the user to change any options for that operation. The user can control one or more operations by selecting them (highlighting one

or more operations) and right clicking (see Figure 0-3). This will produce a popup menu containing the control information for the selected operations (see Table 0-4).

Operation State in the Operation List

Depending on the state of the operation in the operation list, only certain actions are available (see Figure 0-4). The "Initial" state of the operation only occurs when the operation is first added to the operation list (or retrieved from a file). The operation will never go back to the "Initial" State. Once initiated, the operation will stay in the "In Progress" state until one of two things happens, the user cancels the operation, or the operation completes. When the operation enters the "Completed" or "Cancelled" state, the user can re-initiate the operation or delete it from the queue.

| Icon | Description |
|------|---|
| ✓ | Completed – Results are available for the operation. |
| ⌘ | In Progress – The operation is running, no results are available yet. |
| - | Initial – The operation has never been run before (i.e. just add to the operation list). |
| ● | Cancelled - The operation has been cancelled, the results are unavailable. |
| ◆ | Error - An error has occurred with the operation |
| ● | Communication Error - A communication error to the server has occurred, the operation has been cancelled. |

Table 0-5: Status values for each Operation in the Operation List

Icons in the operation list represent the operation status values, see Table 0-5 for a list of the status icons and their description. The results for an operation are only available when the operation is in the "Completed" state. If an operation is selected and its state is not "Completed", the results will be blank. The

"Communication Error" state acts exactly as the "Cancelled" state, but can only be set by the application, and only during a server failure.

vii. Result List



| Column | Description |
|--|---|
| IP Address / Hop | The IP Address of the destination of a ping, or the IP Address of a Hop for a traceroute operation. |
| Sequence | The sequence number of the individual ping or hop in the selected operation |
| Delay (ms) | The delay of the response from the destination, in milliseconds |
| Details  | This button in the details column, will display the Ping List dialog window with the associated traceroute results for that entry displayed in it. It does not appear for ping results. |

Table 0-6: Parameters displayed in the result list for each operation

The result list contains the results from each individual ping or hop in each operation. Depending on what type of operation is selected, the list can contain the list of pings in a selected ping operation (see Figure 0-18), or the list of hops in the selected traceroute operation (see Table 0-6). The title for the IP Address column will change if the operation is a traceroute operation, this column becomes "Hop" (see Figure 0-20). If multiple operations are selected, the result list contains the entries from the first selected operation only. The results appear in order based on the sequence number of each individual ping or hop. If an operation error (i.e. valid diagnostics errors such as Network Unreachable or Node Unreachable for one of the responses) occurs for a Ping operation, the Delay column for that individual entry will display the error.

With a traceroute operation, the number of probes per hop is currently 3. The list of all the delays to that hop can be viewed in a separate window (see Figure 0-5). To display this list window, the user can press the  button (in the

"Detail" column) contained in the row that has more than one delay value (see Figure 0-3). . If an operation error (i.e. valid diagnostics errors such as Network Unreachable or Node Unreachable for one of the responses) occurs for a traceroute operation, the Delay column for that individual entry will display the letter "F" for each packet in the entry. When the user expands the results (i.e. opens the Ping List Window) the actual error will be displayed for each entry in the Delay column. There is a direct relationship between each "F" (failure) and the corresponding entry in the Ping List Window.

| Item | Description |
|--------------|--|
| Highlight | Highlight selected source and destination objects only (see section xxxi). |
| Save Results | Save the results to a user specified file. |
| List LSP | List all known LSPs between the source and destination. |

Table 0-7: Menu items for the result list popup menu

The user can perform actions on each result by selecting it in the result list and right clicking. This will produce a popup menu containing the control information for the selected results (see Table 0-7).

There is no way for IP Maintenance and Diagnostics to highlight the LSP(s) a traceroute or ping operation may go through. Instead, the user can select a specific result entry and execute "List LSP". This will open the List window containing all the known LSPs between the ping source and destination or the selected hop and previous hop for a traceroute operation. This menu item is never disabled, if there are no LSPs between a selected source and destination then the window will appear with no entries.

viii. Response Pane

| Statistic | Description |
|--------------------|---|
| Packet Loss (%) | The percentage of packets sent, that never reached the destination. |
| Jitter (ms) | Variance in delay in individual packets sent to the destination. |
| Maximum Delay (ms) | The slowest response time from the destination. |

| | |
|--------------------|--|
| Minimum Delay (ms) | The quickest response time from the destination. |
| Average Delay (ms) | The average response time from the destination. |

Table 0-8: Statistics displayed for each operation if successful

The response pane contains information about each ping and each hop in a traceroute operation (see Figure 0-6). If the operation is successful, it will display the statistics for the operation (see Table 0-8). If the operation is a traceroute operation, the user must select a specific hop to get the statistics for that hop.

If an execution error has occurred in the operation, the response pane will show the error message (see Figure 0-7) returned from the node and the result list will be empty. An execution error occurs not with an ICMP packet, but an error in the CLI command, such as invalid VRF name. If the results are saved to a local file, the statistics are appended to the end of the file. All operations are logged to a central server file; it includes each packet, the statistics and any errors (see section xxxiv).

IP Maintenance and Diagnostics Scheduling Window

The IP Maintenance and Diagnostics Scheduling window is very similar to the Operation window. It contains 4 areas, Schedule List section, Operation List section, Results section and the Response Pane. The schedule section contains all the schedules in the system. The operation list section contains all the pings available in the selected schedule from the schedule list. To view the summary statistics of an operation from a schedule, the operation must be selected in the operation list.

The result section contains the summary statistics information from the selected operation in the operation list. These statistics include jitter, average delay, and packet loss percentage. The Response pane at the bottom of the window contains any errors associated to the operation (i.e. configuration errors). The Schedule list, Operation List and Result List have scrollbars that appear when the list grows larger than their viewable area. A splitter window that separates the lists also allows the user to choose how large the viewable area is for each

A schedule consists of configured ping operations. The only operation that can be scheduled is the ping operation. Only the Admin can manage schedules (create, edit, delete, acknowledge, enable or disable), everyone else can view the schedules and results as read only, other restrictions can only be applied through scope of command. There can be a maximum of 100 schedules, each containing up to 100 ping operations. A schedule cannot have more than 10 pings per source per minute in one schedule. For example, if the frequency for a schedule is 2 minutes, there cannot be more than 20 pings configured per source in that schedule. This limitation is based on the CLI command and response from the node for pings. This limitation does not take into account timeouts and errors from the ping operations. If an iteration of a schedule is still running and another iteration of the same schedule is supposed to run (e.g. frequency is one minute and the first iteration takes 1minute 10 seconds), it will be skipped.

If a schedule is running, and a user tries to invoke an operation to the same router, they will be warned and the operation will be queued. If a user is

currently performing an operation on a router and a schedule runs with the same source defined, the user operation is cancelled and the user is notified. The schedule has priority at all times. Each schedule is defined by a user-defined name, by default it is date and time of the schedules creation. Schedules can be enable and disabled by selecting the check box beside the associated schedule (see Figure 0-8). To configure a schedule, double click it or select "Schedule->Edit" from the menu.

When a schedule is chosen, the operation list is updated with all the ping operations associated with that schedule. The Status field in the operation list only changes if there is an alarm or error associated to that operation. An operation can be added to a schedule in one of 3 ways:

1. Retrieve operations - Use "File->Open Operations" to retrieve a list of operations from a file to a selected schedule. If the specified file contains traceroute operations, they will be ignored and only ping operations will be retrieved.
2. Create operation - Use the "Operation->New->Ping" to add a new operation to the selected schedule.
3. Drag and drop/Cut, copy and paste operations - Use operations from the Operation window or another schedule and either drag and drop them (move the operations) or cut, copy and paste them into the selected schedule.

The result list contains all the summary information that exists for the selected operation. The summary information includes the time it was calculated, jitter, average delay, minimum delay, maximum delay, packet loss and status. Each summary can be expanded to display all the individual pings that were used to determine that summary information. The Status field in the result list only changes if there is an alarm or error associated to that summary information.

A schedule can associate one alarm for each of the following attributes:

- Jitter (ms)
- Maximum Delay (ms)
- Packet Loss (ms)

The schedule determines if an alarm is generated for one of the attributes by using a threshold. If the summary statistic for that attribute has exceeded the user-specified threshold, an alarm will be raised to the fault management system with the user-specified severity. The calculation is based on a summary period (i.e. a number of summaries). All summary statistics and individual operation results are stored on the server.

The Scheduling window contains common functionality that is used in the Operation window.

ix. Launching IP Maintenance and Diagnostics Scheduling Window

Selecting "Administration->IP Diagnostics Schedule" from the NMS main menu opens the IP Maintenance and Diagnostics client. Restriction of this command is only done through scope of command for the main menu; there are no other restrictions to opening the window. It can be displayed at any time, a router or node does not have to be selected. If a valid router or node is selected when the window opens, it will by default be the specified source object with the name and IP address already filled in for the source field for a ping dialog. If it is an invalid object, the source fields will be blank and the user will have to specify a valid router or node. The user is allowed to open only one scheduling window at a time. If the user selects the IP Diagnostics Schedule menu a second time, and the window is already launched, it will bring it to the front for the user. The IP Maintenance and Diagnostics operation window can also open the schedule window with the "File->Schedule Window" menu item.

x. Status Bar

The status bar is enhanced for the scheduling window. It displays an icon if the scheduler is currently running (i.e. a schedule is currently being processed). The icon only appears on the scheduling window when there is schedule being processed (see Figure 0-8). See section xxiv for a list of the common status bar features.

xi. Menus and Toolbars

| Icon | Menu Item | Shortcut | Description |
|------|-----------|----------|-------------|
|------|-----------|----------|-------------|





| | | Key | |
|---|--------------------------|------|---|
|  | Schedule->New | ? | Create a new schedule (only admin) and display the schedule options dialog. By default, all new schedules are disabled. |
| None | Schedule->Edit | ? | Edit the selected schedules (only admin) parameters through the schedule options dialog. |
| None | Schedule->Enable/Disable | None | Enable/Disable the schedule (only admin) on the server (starts/stops it running) |
| None | Schedule->Delete | None | Delete the schedule (only admin) |
| None | Operation->Acknowledge | None | Acknowledge the alarms associated to the operation (only admin) |
|  | Operation->Refresh | ? | Refresh the summary statistics and status of the selected operations |
|  | File->Operation Window | None | Open the Operation window |
|  | File->Backup Window | None | Open the Schedule Backup window |

Table 0-9: Menu items and associated Toolbar Icons

Common menu items and toolbars are found in Section xxv. The menu items identified in Table 0-9, are specific to the IP Maintenance and Diagnostics Scheduling window.

xii. Saving Summary Results and Individual Results to a Local File
Schedule and operation results can be saved to a local file in one of two formats, CSV or TXT. See section xxvii for a description of the save dialog.

Text Format

Schedule Customer A - VPN1

Ping Toronto - Ottawa Time 12:21pm 2003/01/10

Source138.120.15.90: vrf - vpn1 Destination 13.13.13.2

| Seq | Source | Destination | Delay (ms) |
|-----|---------------|-------------|------------------|
| 1 | 138.120.15.90 | 13.13.13.2 | 112 |
| 2 | 138.120.15.90 | 13.13.13.2 | Node Unreachable |

```
3      138.120.15.90      13.13.13.2      98
```

```
Schedule      Customer A - VPN1
```

```
Ping  Toronto - Ottawa  Status Delay Alarm
```

```
Source138.120.15.90: vrf - vpn1  Destination  13.13.13.2
```

```
Time          12:20pm 2003/01/101
```

```
Jitter (ms)          10.0
```

```
Packet Loss %        0.0
```

```
Average Delay (ms) 10.0
```

```
Maximum Delay (ms)   10.0
```

```
Minimum Delay (ms)   10.0
```

Figure 0-3: Schedule Text Format Example (Ping Detail and Ping Summary)

When the user selects the text format for saving results ("Save as Type" field), it will save it in a standard space formatted file (see Figure 0-3 for an example). The text file will contain either the summary statistics for the selected operations, or the individual results for the selected summaries.

CSV Format

```
Schedule, Customer A - VPN1
```

```
Ping, Toronto - Ottawa, Time, 12:21pm 2003/01/10
```

```
Source, 138.120.15.90: vrf - vpn1, Destination, 13.13.13.2
```

```
Seq, Source, Destination, Delay (ms)
```

```
1, 138.120.15.90, 13.13.13.2, 112
```

```
2, 138.120.15.90, 13.13.13.2, Node Unreachable
```

```
3, 138.120.15.90, 13.13.13.2, 98
```

```
Schedule, Customer A - VPN1
```

```
Ping, Toronto - Ottawa, Status, Delay Alarm
```

```
Source, 138.120.15.90: vrf - vpn1, Destination, 13.13.13.2
```

```
Time, 12:20pm 2003/01/101
```

```
Jitter (ms), 10.0
```

Packet Loss % ,0.0
 Average Delay (ms),10.0
 Maximum Delay (ms),10.0
 Minimum Delay (ms),10.0

Figure 0-4: Schedule CSV Format Example (Ping Detail and Ping Summary)

When the user selects the CSV format for saving results ("Save as Type" field), it will save it in a comma separated formatted file (see Figure 0-4 for an example). The file will contain either the summary statistics for the selected operations, or the individual results for the selected summaries.

xiii. Schedule List

| Column | Description |
|--------------|--|
| Enabled | This is a checkbox to enable or disable each schedule from running |
| Schedule | The unique name of the schedule (see section xviii). |
| Start Time | The start time of the schedule |
| End Time | The end time of the schedule |
| Frequency | The time between each running of the operations |
| Freq. Period | The type of frequency (i.e. days, hours, minutes, etc) |
| Alarm Status | Identifies the highest severity alarm for the schedule (that has not been acknowledged). |
| Status | The status of the schedule, derived from the highest operation status |

Table 0-10: Parameters displayed in the schedule list for each schedule

The schedule list contains the schedules that have been configured in the system. It identifies each schedule by its unique name in the "Schedule" column (see Table 0-10). It allows the user to enable/disable schedules by clicking the checkbox contained in the "Enabled" field associated to the schedule. It also identifies the time and frequency that this schedule is configured with. A schedule can be edited by double clicking the schedule entry in the list, it will then display the schedule configuration window (see section xviii).

| Item | Description |
|--------|--------------------------------------|
| New | Create a new schedule |
| Delete | Delete the schedule(s) from the list |

Table 0-11: Menu items for the operation list popup menu

There is a popup menu that is associated to the schedule list that allows the user to create and delete operations easily (see Table 0-11).

xiv. Operation and Summary Status







| Icon | Description |
|---|--|
|  | Critical Alarm – A critical alarm has been generated based on summary statistics for the operation not meeting the schedules threshold values. |
|  | Major Alarm – A Major alarm has been generated based on summary statistics for the operation not meeting the schedules threshold values. |
|  | Minor Alarm – A Minor alarm has been generated based on summary statistics for the operation not meeting the schedules threshold values. |
|  | Warning Alarm – A warning alarm has been generated based on summary statistics for the operation not meeting the schedules threshold values. |
|  | Error - An error has occurred with the operation in a summary period. |
|  | Normal – The operation has no errors or alarms associated to it. |

Table 0-12: Status values for each Operation in the Operation List

Icons in the schedule list, operation list and result list represent the associated status values; see Table 0-5 for a list of the status icons and their description.

The operation list and schedule list derive their status from the highest status in the summary list.

xv. Operation List

| Column | Description |
|--------------|--|
| Type | The type of operation (see Table 0-14). |
| Name | The Name associated to the operation. |
| Source | The router the operation is being performed on |
| Destination | The object the operation is being performed to |
| Alarm Status | Identifies the highest severity alarm for the schedule (that has not been acknowledged). |
| Status | The status of the operation (see section xiv for a list of status values). |

Table 0-13: Parameters displayed in the operation list for each operation

The operation list contains the list of ping operations contained in a schedule. The operations appear in the order they are added. The status field identifies errors or alarms associated to the operation (see Table 0-13). The status field is derived from the highest alarm in its summary list. The source and destination columns identify the configured source and destination objects for the ping operations. IP Maintenance and Diagnostics Scheduling supports 10 ping operations per minute per node. The maximum number of operations per schedule is 100.


| Icon | Description |
|---|----------------|
|  | Ping Operation |

Table 0-14: Icon representation of the "Type" field in the Operation List

The list will contain all the defined ping operations created by the user and they are distinguishable by the "Type" column (see Table 0-14). Operations in a

schedule may not be done the current iteration before the schedule needs to run again (e.g. based on timeout issues and conflicts with other schedules). If an iteration of the operation is missed due to this, the summary information will have an error status with an error message identifying this summary as "skipped". This may mean the user will have to adjust times or frequencies in this schedule or other schedules. An operation could also have an error status if there was a configuration error (e.g. the specified LSP name has changed on the node).

| Item | Description |
|-----------------|---|
| Refresh | Refresh the summary information for the selected operation. |
| Acknowledge | Acknowledge the alarms and errors associated to the operation |
| Delete | Delete the operation(s) from the list |
| Save Operations | Save the operation(s) for future use |
| Save Results | Save the summary information from the selected operation file (see section xii). |
| Highlight | Highlight all known objects associated with the selected operation (see section xxxi) |

Table 0-15: Menu items for the operation list popup menu

Double clicking on an operation in the operation list will open the appropriate operation window to allow the user to change any options for that operation. The user can control one or more operations by selecting them (highlighting one or more operations) and right clicking. This will produce a popup menu containing the control information for the selected operations (see Table 0-4). The popup menu allows quick access to operations such as refresh for getting the latest results and highlight for highlighting the associated objects. If one or

more alarms have occurred for an operation, the user can acknowledge (clear) the alarms through the popup menu.

xvi. Result List



| Column | Description |
|---|--|
| Time | The time the summary statistics were calculated |
| Packet Loss (%) | The percentage of packets sent, that never reached the destination during the summary period. |
| Jitter (ms) | Variance in delay in individual packets sent to the destination. |
| Maximum Delay (ms) | The slowest response time from the destination during the summary period. |
| Minimum Delay (ms) | The quickest response time from the destination during the summary period. |
| Average Delay (ms) | The average response time from the destination during the summary period. |
| Alarm Status | Identifies the highest severity alarm for the schedule (that has not been acknowledged). |
| Status | The status of the summary (see section xiv for a list of status values). |
| Details  | This button in the Details column will display the Summary Ping List dialog window with the associated individual ping results for the selected summary. |

Table 0-16: Parameters displayed in the result list for each operation

The result list contains the summary results from each operation. If multiple operations are selected, the result list contains the entries from the first selected operation only. The results retrieved for the selected operation are only the ones that exist to that time. If new results come in, the UI will not be updated, but the user can refresh the summary results at any time. The results appear in order based on the time they were calculated (see Table 0-16). The status of the summary could either be normal, an error or an alarm (see section xiv).

With each summary, a list of individual pings is associated to it. These ping values are used when calculating the summary statistics. The list of the entire ping for that summary can be viewed in a separate window (see Figure 0-9). To display this list window, the user can press the  button (in the "Detail" column) contained in the row associated to the summary or double click the

summary. The window will display the time when each ping was performed, the delays associated to each ping and any errors (e.g. Node Unreachable).

Storing all summary and detailed ping information can be quite large. Therefore there are limitations of disk size associated to the IP Diagnostics Scheduling. If the limitation is exceeded, the oldest results for operations will be deleted and will not be retrievable.

| Item | Description |
|--------------|--|
| Save Results | Save the individual ping results to a user specified file (see section xii). |

Table 0-17: Menu items for the result list popup menu

The user can perform actions on each result by selecting it in the result list and right clicking. This will produce a popup menu containing the control information for the selected results (see Table 0-7).

xvii. Response Pane

The response pane only displays execution errors. If an execution error has occurred in the operation or for a specific summary, the response pane will show the error message (see Figure 0-7). An execution error occurs not with an ICMP packet, but an error in the CLI command, such as invalid VRF name, or timing issue with other schedules. All operations are logged to a central server file; it includes each packet and any errors (see section 1.a.xxxiv).

xviii. Schedule Configuration

A new schedule can be created at any time by selecting "Schedule->New. If the parameters are changed for a schedule, they will take effect the next time the schedule runs. This means that any individually calculated threshold value and summary values on the server would be reset, previous results will still be available.

The scheduling configuration window contains 3 tabs, general, schedule and thresholds (see Figure 0-11). This window contains all the necessary fields to configure a schedule.

| Item | Values | Default | Size | Description |
|-----------------------|-----------|--------------------|---------|---|
| Schedule Name | N/A | N/A | 30 Char | The unique identifier (name) of the schedule. |
| Number of Pings | 1 - 255 | 3 | Short | The number of pings to send in a ping operation. |
| Interval (sec) | 1 - 255 | 3 | Short | The time to wait before issuing the next ping. |
| Packet Size (bytes) | 29 - 9192 | 32 | Short | The packet size of each ping. (frozen in this release). |
| Fill Pattern | N/A | 0XAB CDAB CD | 32 bits | The value to pad the ping packet with (frozen in this release). |
| Timeout per Ping (ms) | 0 - 60000 | 20000 | Short | The timeout period to wait for a response (frozen in this release). |
| Type of Service | 0 - 255 | 0 | Short | The type of service, or DSCP bits (frozen in this release). |

Table 0-18: Fields in the General Tab

The fields contained in the general tab are used for basic information identifying the schedule, such as a unique name (see Table 0-18). The ping setting fields are applied to all ping operations contained in the schedule. The fields that apply to pings in the schedule are identical to the standard parameters for normal ping operations. In this release, the values are frozen to the default values.

The schedule tab is used to set the start time, end time and the frequency (in minutes) to run the schedule. This will set the frequency or the number of times the schedule will run (see Figure 0-12).

| Item | Values | Default | Size | Description |
|-----------|------------|------------|------|--|
| Frequency | Per Minute | Per Minute | N/A | The frequency of the schedule (i.e. when it runs). |

| | | | | |
|---------------|----------------|---------------------------|------------|--|
| Process Every | 0 min – 60 min | 15 min | Short | The time between each run of the schedule (increments of 1 minute) |
| Start Date | N/A | Current Date | dd:mm:yyyy | The date for this schedule to start running |
| Start Time | N/A | Current Time | String | The time for this schedule to start running |
| End Date | N/A | Current Date plus one day | dd:mm:yyyy | The date for this schedule to start running |
| End Time | N/A | Current Time | String | The time for this schedule to start running |

Table 0-19: Fields in the Schedule Tab

The frequency field in the schedule tab identifies the time between each run of the schedule. Currently it only allows a frequency from 0 minute to 60 minutes (see Table 0-19). If the user specifies a frequency of 0 minutes, it will only run the schedule once at the specified start date/time, the end date/time are ignored. The start date/time and the end date/time must take the frequency into account. For example, if the start date/time is 2003-02-28 12:10pm, and the frequency is 15 minutes, the end date/time must at least be 2003-02-28 12:25pm. Schedules may overlap; there is no validation between the schedule being configured and existing schedules. This will not be a problem unless the same source router is in more than one schedule that may run at the same time. If schedules run at the same time, the operations contained in those schedules do not have an order, so operations from one schedule could be interspersed with operations from another schedule. If a schedule cannot complete within the specified frequency, the next iteration of the schedule will be skipped. The summary period and individual ping will identify when it has been skipped, by setting the status to "Error" and displaying an appropriate error message. No scheduled ping for a given source router will be able to be executed if another ICMP operation is in progress on the source router. An error will be recorded for that individual ping.

The threshold tab is used to set the threshold values for Jitter, Delay and Packet Loss %.. This will set the summary period as well, the number of iterations that the schedule runs before calculating the summary statistics and creating alarms (see Figure 0-13).

| Threshold | Item | Values | Default | Size | Description |
|-----------------|----------------|---------------------------------------|----------|--------|--|
| N/A | Summary Period | 5 - 1440 | 30 | Short | The number of iterations before calculating the summary statistics. |
| Jitter (ms) | Value | 0 - 60000 | 0 | Short | The maximum variance in milliseconds before a jitter alarm is raised. A specific severity of alarm can be associated to this threshold value. |
| | Severity | Critical Major Minor Warning | Warning | N/A | |
| | (checkbox) | Disabled Enabled | Disabled | N/A | Enables or disables this threshold value. If disabled, the fields become read-only. |
| Delay (ms) | Value | 0 - 60000 | 0 | Short | The maximum delay in milliseconds before a round trip delay alarm is raised. A specific severity of alarm can be associated to this threshold value. |
| | Severity | Critical Major Minor Warning | Warning | N/A | |
| | (checkbox) | Disabled Enabled | Disabled | N/A | Enables or disables this threshold value. If disabled, the fields become read-only. |
| Packet Loss (%) | Value | 0 - 100 | 0 | Double | The number of connectivity failures allowed before a connectivity alarm is raised. A specific severity of |

| | | | | | |
|--|------------|---------------------------------------|----------|-----|---|
| | Severity | Critical Major Minor Warning | Warning | N/A | |
| | (checkbox) | Disabled Enabled | Disabled | N/A | Enables or disables this threshold value. If disabled, the fields become read-only. |

Table 0-1: Fields in the Threshold Tab

The summary period field identifies the number of iterations to wait before calculating summary statistics and determining alarms (see Table 0-1). The minimum summary period is 5 and the maximum 1440. For example, if the summary period is 5 and the frequency for a schedule is 1 minute, then the summary statistics will be calculated after 5 minutes. If an iteration is skipped, then that iteration will not be included in the summary period. Execution errors, such as invalid VRF name, are not used in summary calculations or alarm determination. The threshold fields identify the threshold limit and the associated alarm severity to use if an alarm is raised.

xix. Alarms and Threshold Highlighting

When an alarm is generated for a summary period, that summary and the associated operation have their status shown in the window as an "alarm" state (see section xiv). The user can highlight in the scheduling window the same way as the operation window (see section xxxi). The user can then select any or all operations that have an alarm associated with them and perform "Operation->Highlight". This will highlight all source and destination objects for all the selected operations in a schedule.

For each alarm generated to the NMS fault management system, the following information will be available for each alarm:

- Schedule Name
- Operation Name
- Source Node (VRF and LSP if applicable)

- Destination IP address
- Summary Execution Time
- Threshold that failed (Loss, Jitter, or Delay) - This will be the "probable cause" field in the AS system.
- Threshold value
- Result that caused the threshold failure

The alarm will be raised as a QoS type of alarm. After an alarm has been raised, the user can acknowledge (clear) the alarm in the IP Diagnostics Scheduling window. This will change the status of the operation and the schedule back to a normal state until another alarm is raised. This action is not associated to clearing the alarm in the Fault Management system, it is only associated to the IP Diagnostics Scheduling application. Likewise, with the AS system, If a user clears an alarm it does not clear it in the IP Maintenance and Diagnostics Scheduling application. If a schedule should not raise alarms, the default value of "0" should be used in the fields for the threshold that is not being used. The thresholds are defined by each individual schedule (see section xviii).

xx. Schedule Backups

The schedule backup window is very similar to the regular functionality of the IP Maintenance and Diagnostics Schedule Window. This includes saving results to a local file, copying operations to be used in the Schedule Window or Operation Window, highlighting selected operations, viewing specific detailed results per summary, and viewing the configuration of the stored operations in the operation list. There are only three differences:

1. All operations and schedules are read-only. You can view, but you can not edit.
2. The schedule list contains a list of backup files (many per schedule).
3. Alarms and errors are only visible at the result pane level, they are not visible in the operation or schedule.

There are no restrictions on who can view the schedule backups. There is no limit to the number of backup files for a schedule, the only limitation is disk space.

xxi. Launching IP Maintenance and Diagnostics Schedule Backup Window

The only way to launch the Schedule Backup Window is through the Schedule Window, under "File->Backup Window". There are no restrictions to who can launch this window, the only restriction is based on the scope of command for the Schedule Window. The user is allowed to open only one Schedule Backup Window at a time. If the user selects the menu a second time, and the window is already launched, it will bring it to the front for the user.

xxii. Menus and Toolbars



| Icon | Menu Item | Shortcut Key | Description |
|---|-----------------------|--------------|--|
|  | Schedule->Refresh | ? | Refresh the summary statistics and status of the selected operations |
|  | File->Schedule Window | None | Open the Schedule window |

Table 0-2: Menu items and associated Toolbar Icons

Common menu items and toolbars are found in Section xxv. Any configuration type menu items identified in Section xxv do not apply to this window. The menu items identified in Table 0-9, are specific to the IP Maintenance and Diagnostics Scheduling Backup window.

xxiii.Redundancy

The Active NMS machine contains the main repository for summary and operation results. The repository is copied to the Standby NMS in case of Active failure. The repository is synchronized between the active and standby. In the event of a switch over the clients will switch over to the Standby (or new active) to retrieve the summary and operation results. The backup directory is not synchronized between the active and standby, this must be done by the customer.

Common IP Maintenance and Diagnostics Functionality

This section describes common functionality used by both the IP Maintenance and Diagnostics Operation Window (see Figure 0-3) and the IP Maintenance and Diagnostics Scheduling Window (see Figure 0-8).








xxiv. Status Bar

The main window contains a status bar at the bottom. The status bar displays the number of operations in the operation list and status messages. These status messages depend on the operation that is currently selected. It is a description of the current state the operation is in. For example, if an operation has been initiated but no response is back, it will display the message "In Progress...".

xxv. Multi-Column Sorting

All tables in the Operation and Scheduling windows allow sorting by columns. Each table can be sorted by multiple columns, in ascending or descending order. Clicking the header of a column will sort it in ascending order, clicking it a second time reverse the order. As columns are clicked, they will be sorted in the order they are clicked, with the last column being the first column sorted. To remove a column from the sort, hold the ctrl key and click the column to remove, it will no longer be included in the table sort.

xxvi. Common Menus and Toolbars

| Icon | Menu Item | Description |
|---|--------------------------------|---|
|  | File->Save Result <u>A</u> s | Save results from an operation to a file as text or CSV format. |
|  | File-> <u>S</u> ave Operations | Save the Operation List. |
|  | File-> <u>O</u> pen Operations | Retrieve the Operation List. |
|  | <u>E</u> dit->Cut | Cut the operation |
|  | <u>E</u> dit->Copy | Copy the operation |
|  | <u>E</u> dit->Paste | Paste the operation |
|  | Operation->New->Ping | Open the Ping window for creation. |
| None | Operation->Edit | Edit the selected Operation |




| | | |
|---|----------------------|---|
|  | Operation->Highlight | Highlight the selected operation. |
|  | Operation->Delete | Delete the operation from the Operation List. |
| None | Result->Highlight | Highlight the selected result from the operation. |
|  | Help | Display the help window for IP Diagnostics. |
| None | File->Exit | Exit the IP Diagnostics Application. |

Table 0-3: Menu items and associated Toolbar Icons

Table 0-1 above describes the functionality associated with each menu item, its toolbar icon, and its shortcut key. Some of the menu items are available in popup menus on the operation, schedule and result list. All dialogs opened in the IP Maintenance and Diagnostics windows are modal to that window only, and will not disable any other application.

xxvii. Saving Results to a Local File

Operation results from one or more operations/schedules can be saved to a local file. It allows the user to select one or more of the objects and save the results to a file. The user can choose the directory and file name, along with one of two file formats, Text and CSV. The default directory when the window is opened is the user home directory and the default file type is CSV. If the user selects an existing file, it will notify the user that the file exists, and ask if they wish to overwrite it. The format of the results from the scheduling window and the operation window are different, refer to section xii for an example from scheduling window and section v for an example from the operation window.

xxviii. Retrieving an Operation List

The entries in the Operation List can be retrieved from a user-specified file. To retrieve a saved operation list, select "File->Open Operations" from the main menu. A dialog will appear (see Figure 0-16) that will allow the user to specify a file containing an operation list. The file type is a specific one to the client, and cannot be manually edited by the user, so the "File of Type" field is frozen

to this value. Once the file is specified, the operation list will be updated to contain the operations from the file and the existing operations. The values are not validated at the time the file is loaded only when the operation is initiated or the schedule runs. The default directory when the window is opened is the user home directory.

In the Operation window, the status field will be blank, as it appears when an entry is first manually added to the list through the client, until the operation(s) are initiated at least once. The last results for the retrieved operations are not available and will appear blank if an operation is selected before it has been initiated at least once.

In the Scheduling window, the operations will be retrieved to the currently selected schedule. The summary results and status will be blank until the schedule runs at least one time.

xxix. Save an Operation List

The entries in the operation list can be saved to a user-specified file. To save an operation list, select the operations to save and select "File->Save Operations" from the menu. A dialog will appear (see Figure 0-17) that allows the user to specify a file to save the operation list to. The default directory when the window is opened is the user home directory. If a file exists with the name specified, it will ask the user for verification that they want it overwritten. After the user selects "Save", the file will be updated to contain the operations selected by the user, including any parameters to the operations. The file is a specific type to the client and cannot be edited manually by the user. Only the configuration of each operation is saved, the status and results are not stored in the file. Once the operations are saved to a file, they can be used on other workstations. The file must be transferred manually by the user to the other workstation, but once it has been transferred, the client on that workstation can then retrieve the list of operations.

In the Operation window, if the user closes the client, and the operation list has changed since the last save, it will popup a warning message and allow them to save the operation list before exiting the client.

xxx. Valid Source and Destination Objects

The source and destination objects are specified in the appropriate operation window. Both ping and traceroute have the same valid source and destination objects.

Source

The source field is used to define what router the ping or trace route operation is coming from. The following is a list of valid objects that could be specified in the source fields:

- Router
- Router Interface (the source endpoint identifies the source router and VRF name if one is specified)
- Node
- First Hop LSP (the source router will be determined by the source endpoint of the LSP)

If a supported Router or Node is specified as the source, then the VRF Name can be specified. This field is not enabled if a first hop LSP is selected as the source first (i.e. an LSP and VRF name can not be specified at the same time).

To specify a router, node or LSP, the user can select it in another application (i.e. make it the selected object) and paste it in (see Figure 0-3). If an invalid object is selected, an error message is displayed to the user. If it is an LSP that is pasted in, the Router and IP Address fields will be filled with the information from the source endpoint of the LSP. This includes the management IP address and name of the source Router.

Selecting a router interface and pasting it in can specify the source router or node. It will automatically fill in the associated IP Address and Router name. If a VRF name is associated to the router interface, it will automatically fill in the VRF name.

Another way to specify a router or a node is to query on the management IP Address. The user can enter the IP Address in the IP Address field and then press "Enter". If this is the management IP address of a supported router or node, its name will be filled in. If it is an unsupported node or router, an error message is displayed to the user.

The user can specify a VPN by filling in the VRF name in the source field. A valid router or node must also be specified. The NMS does not validate the name, instead it will be done at the time the operation is initiated on the router. If the router finds a problem with the specified VRF name, an error will be displayed to the user in the response area. A VRF name cannot be selected at the same time as the LSP.

The object type that is being used to define the source must have the radio button selected beside the type. For example, if the source is defined by the LSP, the radio button beside the LSP field must be selected. The radio button selection defines which fields are enabled for that object type.

Destination

The destination fields are used to define what object the ping or trace route operation is going to. The following is a list of valid objects that could be specified in the destination fields:

- Any IP address (whether it is a NMS managed object or not)
- Router ID (Router managed by the 5620)
- Node (specified with an IP Address)

Pasting in one of the following objects known to the NMS can also specify a destination:

- Router Interface (the destination endpoint will be the router interface IP address, in the case of unnumbered, it is the router ID)
- LSP (the destination router will be determined by the destination endpoint of the LSP)

To specify an object by IP Address or Router ID, enter the value in the IP Address field. If this is a Router ID of an object that the NMS is managing, its name will appear in the destination field. If it is an IP Address, the destination

field will say "Unknown". To specify a node that isn't in the list of supported nodes/routers (e.g. 7470) the user must enter the IP address of the destination object. There is no support for pasting in an object that does not have routing capabilities.

To specify a router, node, router interface, or LSP, the user can select it in another application (i.e. make it the selected object) and paste it in (see Figure 0-3). This action will also fill in the IP Address field with the objects IP Address, or in the case of a router or node, the Router ID. If it is a router interface, it will fill in the Router ID and IP Address of the router the interface is on. If it is an LSP, it will fill in the Router ID and IP Address of the destination endpoint of the LSP. If an invalid object is selected, an error message is displayed to the user.

The object type that is being used to define the destination must have the radio button selected beside the type. For example, if the destination is defined by the LSP, the radio button beside the LSP field must be selected. The radio button selection defines which fields are enabled for that object type.

xxxi. Drag and Drop/Cut, Copy, and Paste

Operations can be moved from the operation window to the scheduling window (and between schedules) by one of 2 methods, Drag and Drop and/or Cut, Copy and Paste. The Drag and Drop method allows the user to select multiple operations, click the mouse and drag those selected operations to the other window. The Cut, Copy and Paste method allows the user to select multiple operations, click a cut/copy menu item (see section xxv) and then paste on the other window. Valid windows to select operations are the operation lists in the scheduling window or the operation window. Valid drop areas are the operation lists in the scheduling and operation window, or a schedule in the schedule list window. Currently the only supported operation is the ping operation. If the user tries any other type of operation an error will be displayed.

xxxii. Highlight

Ping and Traceroute operations can be highlighted using the existing highlight functionality in the 5620. Any objects managed by the NMS can be highlighted, including routers, nodes and IP Links. Any NMS application that supports highlighting will highlight the objects specified by the user in the IP Maintenance and Diagnostics application. These applications include but are not limited to the IP Map, NMS Map, Object Navigator, and the listing tools. All highlight operations in the IP Maintenance and Diagnostics window are performed through either the operation list popup menu, or the result list popup menu (see sections vi and vii respectively, for information about the popup menus). However, depending on what the selected operation is, different objects will be highlighted. For the operation list, the following objects are highlighted based on the operation:

- Ping - The source and destination objects are highlighted (i.e. Router and Node).
- Traceroute - The source object, destination object, and all the hops between (including the IP Links) are highlighted (i.e. Router, Node, and IP Link).

For example, highlighting a traceroute operation that contained the following:

| | | | |
|----------------|---------------|---------------|----------------------|
| Source:1.1.1.1 | Hop1: 2.2.2.2 | Hop2: 3.3.3.3 | Destination: 4.4.4.4 |
|----------------|---------------|---------------|----------------------|

Would highlight the source Router, the IP Link, and Router to hop1, the IP Link, and Router to hop2, and then the IP Link, and Router at the destination (this includes all parent objects, such as Nodes).

If a specific entry in the result list is selected and "highlighted", and it is an object that is managed by the 5620, the selected entry, if managed by the 5620, will be highlighted. If a VRF name is specified in the operation, it will be used when determining what objects to highlight. This will only affect the IP Link that is highlight going to the customer edge. If an LSP is defined in the operation, it will not be highlighted. The source and the LSP's associated destination (if managed by the 5620) will be highlighted. In the case of a

traceroute, the hops that are contained within an LSP will not show up in the results, and will not be highlighted. Any hops outside of the LSP will be highlighted. There is no highlighting of objects inside the IP Maintenance and Diagnostics window.

xxxiii. Operations

This section contains definitions of all operations supported by IP Diagnostics and Maintenance.

Ping Operation

The ping operation is used to check network connectivity between the source and destination (see Figure 0-18). The source is where the ping is being initiated from (see section 0 for a list of valid sources) and the destination is where the ping is being sent to (see section 0 for a list of valid destinations).

To create a ping operation, select "Operation->New->Ping" from the menu (or the shortcut identified in Table 0-1). It will open the Ping Operation dialog (see Figure 0-19). From here the user can specify all the parameters for the ping operation.

| Item | Value s | Default | Size | Description |
|------------------------|--------------|-------------------------------|---------|---|
| Name | String | Full Name of source router | 32 | Name for the ping operation |
| Source | N/A | (see section iii) | N/A | The router the operation is coming from. |
| Destination | N/A | N/A | N/A | The object the operation is going to. |
| Number of Pings | 1 - 255 | 3 | Short | The number of pings to send in a ping operation. |
| Interval (sec) | 1 - 255 | 3 | Short | The time to wait before issuing the next ping. |
| Packet Size (bytes) | 29 - 9192 | 32 | Short | The packet size of each ping. (frozen in this release). |
| Fill Pattern | N/A | 0XABCDABC D | 32 bits | The value to pad the ping packet with (frozen in this release). |

| | | | | |
|-----------------------|-----------|-------|-------|---|
| Timeout per Ping (ms) | 0 - 60000 | 20000 | Short | The timeout period to wait for a response (frozen in this release). |
| Type of Service | 0 - 255 | 0 | Short | The type of service, or DSCP bits (frozen in this release). |

Table 0-4: Fields displayed for each ping operation

The parameters that can be filled in for each ping operation is standard options, such as "Number of Pings" and "Type of Service" (see Table 0-4 for a list of all the parameters). Once the source, destination, and parameters are specified, the ping can then be added to the operation list by clicking the "Add" button. The ping does not automatically start once its added to the list, it must be "initiated" before it will try and execute the operation on the router (see section vi for a description of the operation list). Once the ping is complete, the results are displayed in the result list and response pane (see sections vii and viii respectively). The results displayed for a ping operation are not saved by the 5620, if the user does not save the results to their local workstation, they will be lost when the client closes or the operation is initiated again.

The result list contains each individual ping that was sent in the selected ping operation. It displays specific information such as delay and ping sequence number for each individual ping. The response pane will display statistics associated with the entire ping operation. If the ping is not yet complete, the response pane will display an "In Progress..." message to the user in the progress bar. The user can change the parameters associated to a ping operation only when the operation is not in progress, by double clicking it in the operation list, or selecting it and executing "Operation->Edit". This will open the Ping window with the values associated to that operation and allow the user to change any of the parameters associated to the selected operation.

Traceroute Operation

The traceroute operation is used to determine the route taken by packets from a source to a particular host (see Figure 0-20). The source is where the traceroute

is being initiated from and the destination is where the traceroute is being sent too.

To create a traceroute operation, select "Operation->New->Traceroute" from the menu (or the shortcut identified in Table 0-1). It will open the Traceroute Operation dialog (see Figure 0-21). From here the user can specify all the parameters for the traceroute operation.

| Item | Values | Default | Size | Description |
|---------------------|-----------|----------------------------|-------|---|
| Name | String | Full Name of source router | 32 | Name for the ping operation |
| Source | N/A | (see section iii) | N/A | The router the operation is coming from. |
| Destination | N/A | N/A | N/A | The object the operation is going to. |
| Source | N/A | (see section iii) | N/A | The router the operation is coming from. |
| Destination | N/A | N/A | N/A | The object the operation is going to. |
| Maximum TTL | 0 - 64 | 30 | Short | The maximum time to live (frozen in this release). |
| Probes per Hop | 3 | 3 | Short | The number of "pings" to each hop in the route (frozen in this release). |
| Interval (sec) | 1 - 255 | 3 | Short | The time to wait before issuing the next traceroute (frozen in this release). |
| Packet Size (bytes) | 29 - 9192 | 32 | Short | The packet size of each probe (frozen in this release). |

| | | | | |
|------------------------|-----------|----------------|------------|---|
| Fill Pattern | N/A | 0XABCDABC D | 32 bits | The value to pad the packet with (frozen in this release). |
| Timeout per Probe (ms) | 0 - 60000 | 3000 | Short | The timeout period to wait for a response (frozen in this release). |
| UDP Port | 0 - 65535 | 33434 | Short | The port to send the traceroute to (frozen in this release). |

Table 0-5: Fields displayed for each traceroute operation

The parameters that can be filled in for each traceroute operation are standard options, such as, "Probes per Hop" and "UDP Port" (see Table 0-5 for a list of all the parameters). Once the source, destination, and parameters are specified, the traceroute can then be added to the operation list by clicking the "Add " button. The traceroute does not automatically start once it's added to the list; it must be "initiated" before it will try and execute the operation on the router (see section vi for a description of the operation list). Once the traceroute is complete, the results are displayed in the result list and response pane (see sections vii and viii respectively). The results displayed for a traceroute operation are not saved by the 5620; if the user does not save the result locally, they will be lost when the client closes or the operation is initiated again.

The result list contains each individual hop that was sent in the selected traceroute operation. It displays specific information such as delay for each individual hop. The response pane will display statistics associated to each individual hop (i.e. the currently selected hop) in the traceroute operation. If the traceroute is not yet complete, the response pane will display an "In Progress" message to the user in the status bar. The user can change the parameters associated to a traceroute operation only when the operation is not in progress, by double clicking it in the operation list, or selecting it and executing "Operation->Edit". This will open the Traceroute window with the

values associated to that operation and allow the user to change any of the parameters associated to the selected operation.

xxxiv. Historical Log

The results from all operations are logged by the server to a log file. Every time a schedule is run on the server, it identifies it in the log file. This file cannot be displayed through the client, but is available to the user on the server host in a text file. The log contains the main log, and a backup. When the main log grows to the maximum size, it is copied to a backup and the main log will be cleared. The files can grow very large over time; hence they are restricted to a set amount of disk space. If the files grow too large, the oldest results are deleted to make space for the new results (i.e. the backup file is overwritten). However, the size of the files is configurable for each server. If a switchover happens from the active to the standby, the history log is not copied to the standby workstation.

Standard CORBA Interface to Other Applications

The control of the ping and traceroute operations as well as the scheduled operations, to the source routers resides in an IP Maintenance and Diagnostics server. This process contains the control to the router(s) for issuing the operations. This allows rules associated to each type of router to be removed from the client, making the server a common interface to all supported routers

The interface used by the IP Maintenance and Diagnostics client is a CORBA interface (see Figure 0-22) that gives other applications the ability to use the services provided by the IP Maintenance and Diagnostics server. Using CORBA as the interface between a client and the server allows a generic communication without having to understand where the server is in a distributed network or what the specific interface to the server process looks like. The server will make public only the Ping, Traceroute, and Scheduling interfaces. The public interface to the server could be made public in the future for customer use, but security issues may affect this.

Performance

This feature will have an effect on performance. Each individual ping or traceroute on a router will not affect performance of the UI or the server.

However, if many operations are queued on the server or multiple schedules are running, going to multiple nodes, it will affect the performance of the server.

Scalability

The performance issue effects scalability in the number of ping/traceroute requests that can happen to the same router. It is also affected by the configuration of the schedules. Multiple schedules running at the same time will queue operations to routers and may result in iterations of the schedule being missed. This will have to be monitored by the users. Any missed iterations will be identified in each summary period. There is, at most, only one active session to a router at one time. This will restrict users from accessing the same router at the same time.

The operations are sent to the routers through CLIP and are queued on a router basis in CLIP. The limitation is from CLIP to the Router, only one active diagnostic session is allowed currently between CLIP and the router. CLIP will not stop other types of operations to the node (i.e. reconcile and configuration scripts) while diagnostics operations are in progress. All operations going to the same router in CLIP are queued and will be sent in order to the router, there is no concept of priority of the operations.

To increase scalability in the future, more support is needed from the nodes and CLIP. The ability to send multiple operations at one time without logging in for each operation and the ability to perform background operations such as ping will increase the scalability of the server.

Risk

This feature adds the ability for clients to send ICMP packets to routers in a network. There is some risk to sending these type of messages, without control it can affect performance on the routers. Ping is well known for denial of service attacks, where the number of pings and amount of data can slow down or stop any response from the routers. An attacker may also use these operations to find out the topology and vulnerabilities in the Network. There is security from the NMS perspective, which includes scope of command and the server queue where only one ping can be performed on the same router at one

time (i.e. as soon as the first ping is complete on a router, the second can start on that same router). However, this does not prevent a ping command from containing harmful parameters such as a large interval or large packet size. In this release it will not be an issue as the ICMP parameters are frozen and are not configurable.

EVOLUTION OF FUNCTIONALITY

Future Functionality

xxxv. Individual Ping Parameters per Schedule

Currently, the ping parameters are associated to all the ping operations in the schedule. It would be useful to associate the parameters per ping in the schedule.

xxxvi. Multiple operations in one session

The ping and traceroute operations to the node currently use a separate session into the node. This means each operation must connect, login, execute the command and logoff. It would improve performance if there were a way to connect, login, execute a series of operations and then logoff.

xxxvii. Scheduled Traceroute

The only operation that can be currently scheduled is the ping operation. There may be a need in the future to schedule traceroutes as well.

xxxviii. Ping and Traceroute from source NMS

Allow a network management station to perform a ping or traceroute. This would allow the users to test connectivity from network management stations.

xxxix. Hostname DNS lookup

In the future, it would be good to allow the user to specify a hostname and automatically lookup the IP Address from a DNS server. This would allow for pings and traceroute operations to publicly visible destinations.

xl. CVS control for historical logs

Adding the historical logs to a repository such as CVS. This could be added to change management for control of these historical logs.

xli. Central Repository for Operation Lists

Adding a central repository to store and version control operations lists (i.e. Change Management) would help users so they don't have to control where their operation list file is located and it is accessible from different machines.

REQUIREMENTS

| Rq't # | Requirement |
|---------------|---|
| R1361-1.2.3.4 | <p>NMS shall allow the user to print results for operations in a schedule.</p> <p>The results will be printed in text format.</p> |
| R1361-1.2.3.5 | <p>NMS shall allow the user to print information on selected schedules.</p> <p>The information for a schedule includes start/end times, threshold values and a list of its operations.</p> |
| R1361-1.2.5.3 | <p>NMS shall allow profiles (sets) of alarm thresholds to be created and associated to one or more scheduled matrix of ping operations.</p> <p>Each profile can contain zero or more alarm thresholds for jitter, delay or loss. Each defined threshold will have an associated alarm priority. A schedule can only be assigned to one alarm threshold profile.</p> |
| R1361-1.2.5.4 | <p>NMS shall allow users to highlight the Ping sources which do not meet the following user specified thresholds:</p> <ul style="list-style-type: none"> • Delay Threshold • Jitter Threshold • Loss Threshold <p>Highlighting is not automatic; it will be a separate step that the users have to initiate.</p> |
| R1361-1.2.5.6 | <p>NMS shall allow users to highlight the affected Node from the AS system.</p> <p>Highlighting is not automatic; it will be a separate step that the users have to initiate.</p> |

FURTHER REQUIREMENTS

| Rq't # | Requirement |
|------------------|--|
| R1317-1.1.11 | <p>NMS shall allow users to define a set/matrix of network points between which continuous background Ping operations will be executed.</p> <p>See R1317-1.4 for scalability limitation.</p> |
| R1317-1.1.11.1 | <p>NMS shall allow users to specify a set of Ping sources and Ping targets for Ping operations.</p> <p>The Ping parameters as specified in R1317-1.1.7 – R1317-1.1.8 will be common to all the combination of Ping operations generated from the matrix.</p> |
| R1317-1.1.11.2 | NMS shall allow users to specify multiple sets of Ping matrix. |
| R1317-1.1.11.3 | <p>NMS shall allow users to specify a schedule for the Ping matrix. The schedule may include one or a combination of the following:</p> <ul style="list-style-type: none"> • 'Now' or 'Date and time' the Ping operations are to be carried out • 'Once only' or 'the interval' (e.g. every N x 15 minutes or every N hour after) at which the Ping operations are to be carried out |
| R1317-1.1.11.3.1 | <p>NMS shall prevent users from scheduling over-lapping matrices that may result in > 255 Ping commands being issued by the NMS at the same time.</p> <p>This is regardless of whether the commands are issued to the same or different Ping source.</p> |
| R1317-1.1.11.4 | The results as specified in R1218-1.1.9 shall be available for each of the Ping operations generated from the Ping matrix. |
| R1317-1.1.11.5 | <p>NMS shall allow users to highlight the Ping sources which do not meet the following user specified thresholds:</p> <ul style="list-style-type: none"> • X number of connectivity failures over Y timeframe • Round Trip Delay Threshold • Jitter Threshold <p>Highlighting is not automatic; it will be a separate step that the users have to initiate after the Ping operation is completed.</p> |
| R1317-1.1.11.6 | <p>NMS shall allow users to enable alarm generation for Ping sources which do not meet the following user specified thresholds:</p> <ul style="list-style-type: none"> • X number of connectivity failures over Y timeframe • Round Trip Delay Threshold • Jitter Threshold |

- R1317-1.2.9 NMS shall display the following non-configurable Traceroute parameters in the Traceroute operation user interface:
- Maximum TTL
 - Probes per hop
 - Packet Size
 - Time to wait before timing out per probe sent
 - Data fill Pattern
- UDP Port
- R1317-1.4 NMS shall achieve the following scalability and performance targets:
- Support up to 255 concurrent Ping and Traceroute operations at a time regardless of whether the operations are issued to the same or different Ping/Traceroute sources.
 - NMS shall not block the graphical user interface for more than 5 seconds after a user issues a Ping or Traceroute request.
- Results may be displayed after a longer period of time depending on either the timeout set by the users or the response from the 7670 node, whichever happens first.
- R1317-1.4.2
- Support up to 64 Ping matrix in the NMS system
 - Support up to 255 entries in each Ping matrix
- R1317-1.5 NMS shall provide an API for the Ping and Traceroute operations to other processes.

[69] Advantages provided by the proposed solution include

1. A simple solution to implement on a Network Management System because provisioning of the connectivity verification tests are centralized and do not require manual logging-on the particular source network nodes.
2. The solution provides schedule connectivity verification testing to be executed periodically, which saves the operator's time, thereby reducing a service provider's operating costs.
3. The solution increases the reliability, availability and serviceability of the IP connectivity by providing immediate alarms and results to be summarize for later analysis.

4. The solution enhances and simplifies the IP diagnostics and maintenance capability for solving service provider network problems. It also allows the customer to test the network provisioning prior to enabling a data service.
5. Because the management is done through a GUI associated with the NMS system, the configuration is much easier than using the legacy CLI on a per source network node (router) basis, which is error prone.
6. A further advantage includes being able to view/configure/modify/store the 'N' network connectivity verification tests and provide the resulting information immediately (through views or alarms) or historically in a network management context.

[70] Reducing operating expenditures is important service providers. The invention automates the diagnostics process of creating and maintaining connectivity test, thereby reducing the operating costs of carrying out these functions. This also ensures that IP connectivity meets the customer expectations as far a jitter, delay and loss of data. Furthermore, the invention reduces operating costs and increases reliability, both of which are valuable to service providers.

[71] The embodiments presented are exemplary only and persons skilled in the art would appreciate that variations to the above described embodiments may be made without departing from the spirit of the invention. The scope of the invention is solely defined by the appended claims.

WE CLAIM:

2. A network management connectivity verification framework comprising:
 - a. a connectivity verification server performing unattended connectivity verification jobs; and
 - b. a connectivity verification application for defining connectivity verification jobs, configuring the connectivity verification server accordingly, and displaying configuration verification results.
3. A connectivity verification framework claimed in claim 1, wherein the connectivity verification jobs are scheduled and the connectivity verification server performs scheduled connectivity verification.
4. A connectivity verification framework claimed in claim 1, wherein the connectivity verification application further providing a display of connectivity verification results.
5. A connectivity verification framework claimed in claim 1, wherein the results of each connectivity verification job may be compared against a connectivity profile, a deviation from the connectivity profile being used to raise an alarm.
6. A connectivity verification framework claimed in claim 4, wherein the connectivity verification results, including alarm information, are further used to generate a network map displaying selected connectivity verification results.
7. A method of creating a network connectivity verification test, comprising steps of:
 - a. defining a connectivity verification job;
 - b. configuring a connectivity verification server to perform the connectivity verification job; and

- c. displaying connectivity verification results.
8. The method of creating a network connectivity verification test claimed in claim 6, wherein defining the connectivity verification job further comprises steps of:
 - a. selecting via an NMS GUI, a pair of source and destination IP objects between which connectivity is to be verified; and
 - b. specifying a connectivity verification schedule;
 9. The method of creating a network connectivity verification test claimed in claim 7, wherein defining the connectivity verification job further comprises steps of:
 - a. specifying connectivity verification thresholds to be applied against connectivity verification results.
 10. The method of creating a network connectivity verification test claimed in claim 8, wherein specifying connectivity thresholds further comprises specifying a threshold for a round trip delay, jitter, and packet loss.
 11. The method of creating a network connectivity verification test claimed in claim 7, wherein a selected IP object include one of a router, IP interface, and IP address
 12. The method of creating a network connectivity verification test claimed in claim 7, wherein the pair of IP objects is selected selecting one of an IP link, an LSP, and a VPN.
 13. The method of creating a network connectivity verification test claimed in claim 6, wherein defining the connectivity verification job further comprises a step of: configuring a connectivity verification parameter including one of a number of ping commands to issue, a ping packet size, ping data fill pattern, a time to wait for response, and a type of service.

14. The method of creating a network connectivity verification test claimed in claim 6, wherein defining the connectivity verification job further comprises a step of: configuring a connectivity verification parameter including one of a number of traceroute commands to issue, a traceroute packet size, traceroute packet data fill pattern, a time to wait for response, and a type of service.
15. A method of performing a network connectivity verification in a network management context comprising steps of:
 - a. performing scheduled connectivity verification;
 - b. comparing a connectivity verification result with a threshold; and
 - c. raising an alarm if the connectivity verification result has reached the threshold.
16. The method of performing a network connectivity verification claimed in claim 15, further comprising a step of: storing connectivity verification job on computer readable medium for subsequent access and execution.
17. The method of performing a network connectivity verification claimed in claim 15, further comprising a step of: highlighting at least one IP object based on one of a connectivity verification job and a connectivity verification result.
18. The method of performing a network connectivity verification claimed in claim 17, wherein a highlighted object is one of an OSI Layer 2 and OSI Layer 3 object.
19. The method of performing a network connectivity verification claimed in claim 15, wherein performing scheduled connectivity verification the method further comprising a step of: periodically executing connectivity verification tests.

20. The method of performing a network connectivity verification claimed in claim 15, wherein performing scheduled connectivity verification the method further comprising a step of: issuing a one of a ping command and traceroute command.
21. The method of performing a network connectivity verification claimed in claim 15, further comprising a step of: storing historical connectivity verification results on computer readable medium for subsequent access.

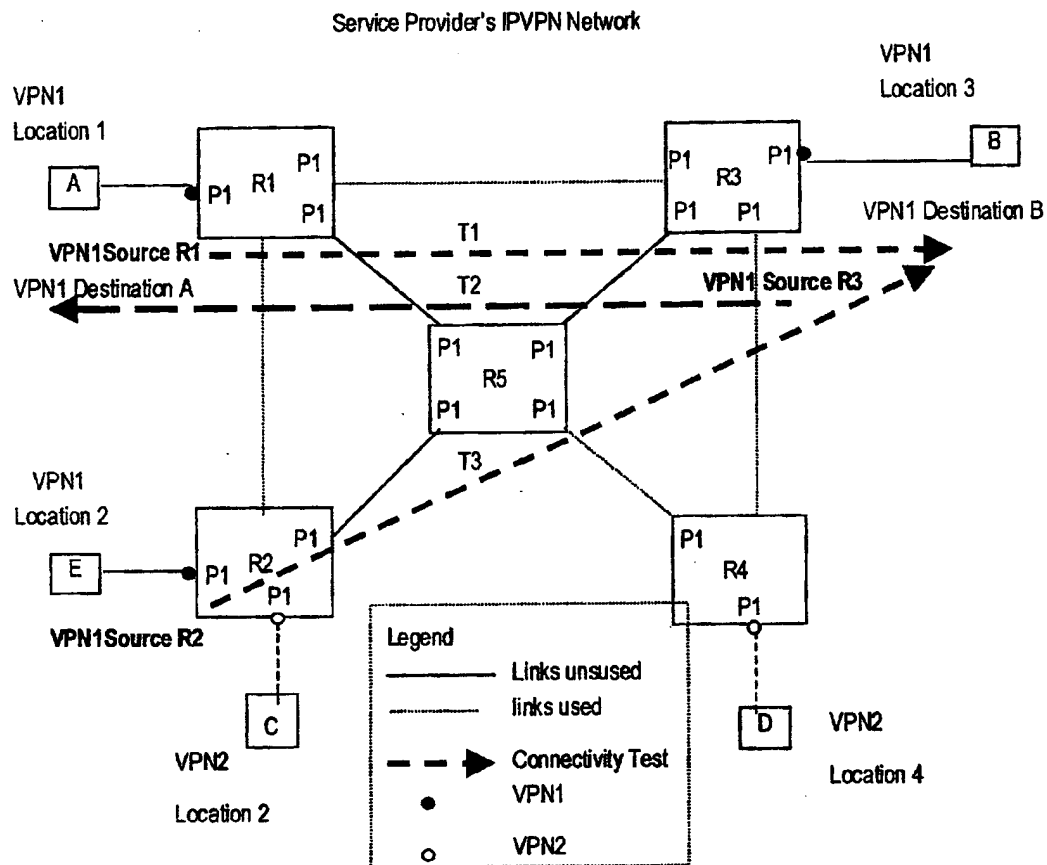
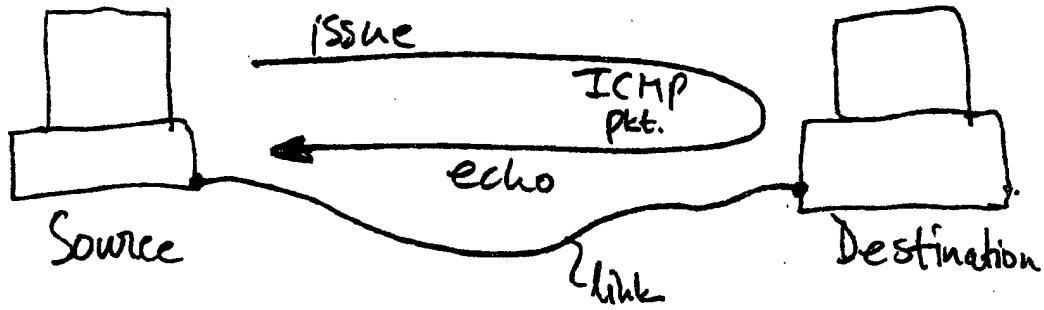
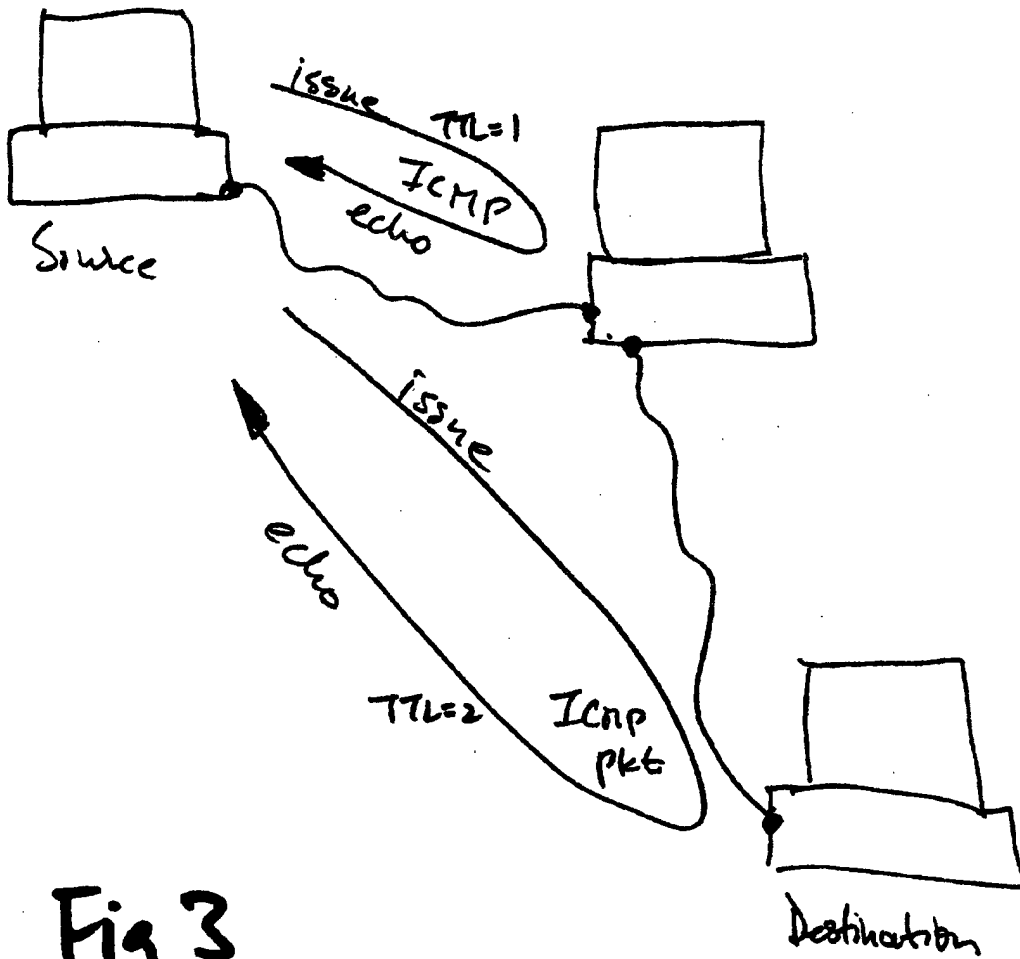
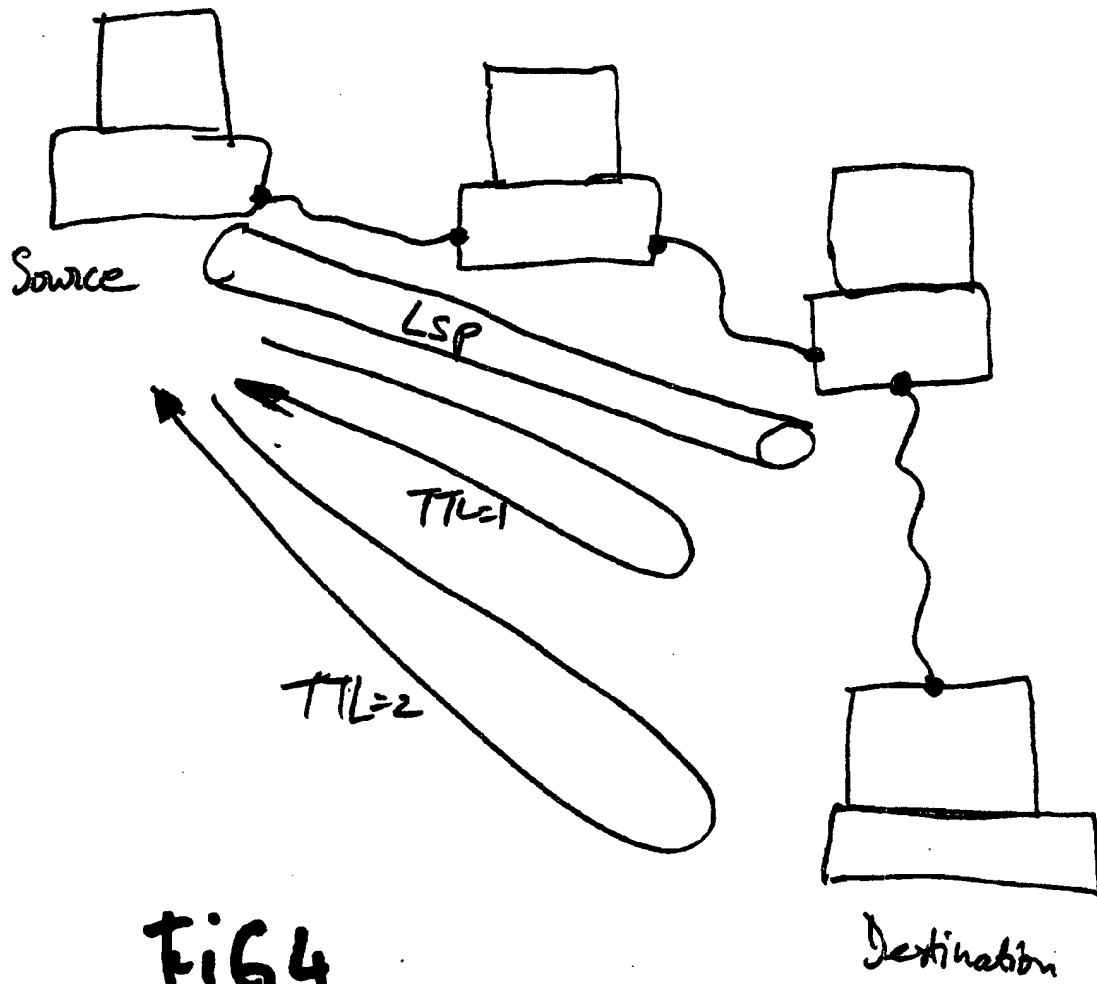


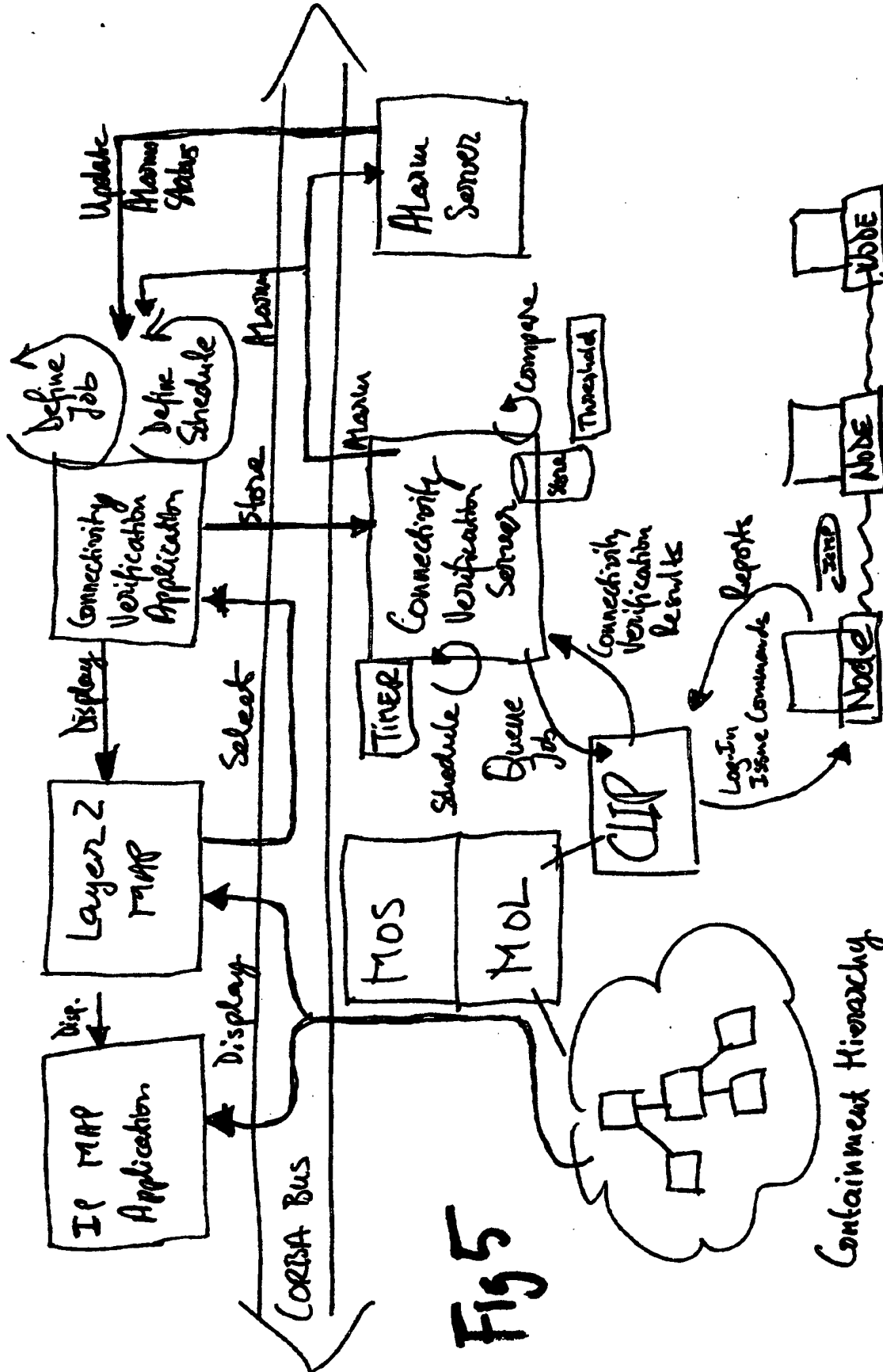
Figure 1 Prior Art

Mark A. Oles

**FIG 2.****Fig 3***Marks & Clerk*



Marks & Clerk



Marks & Clerk

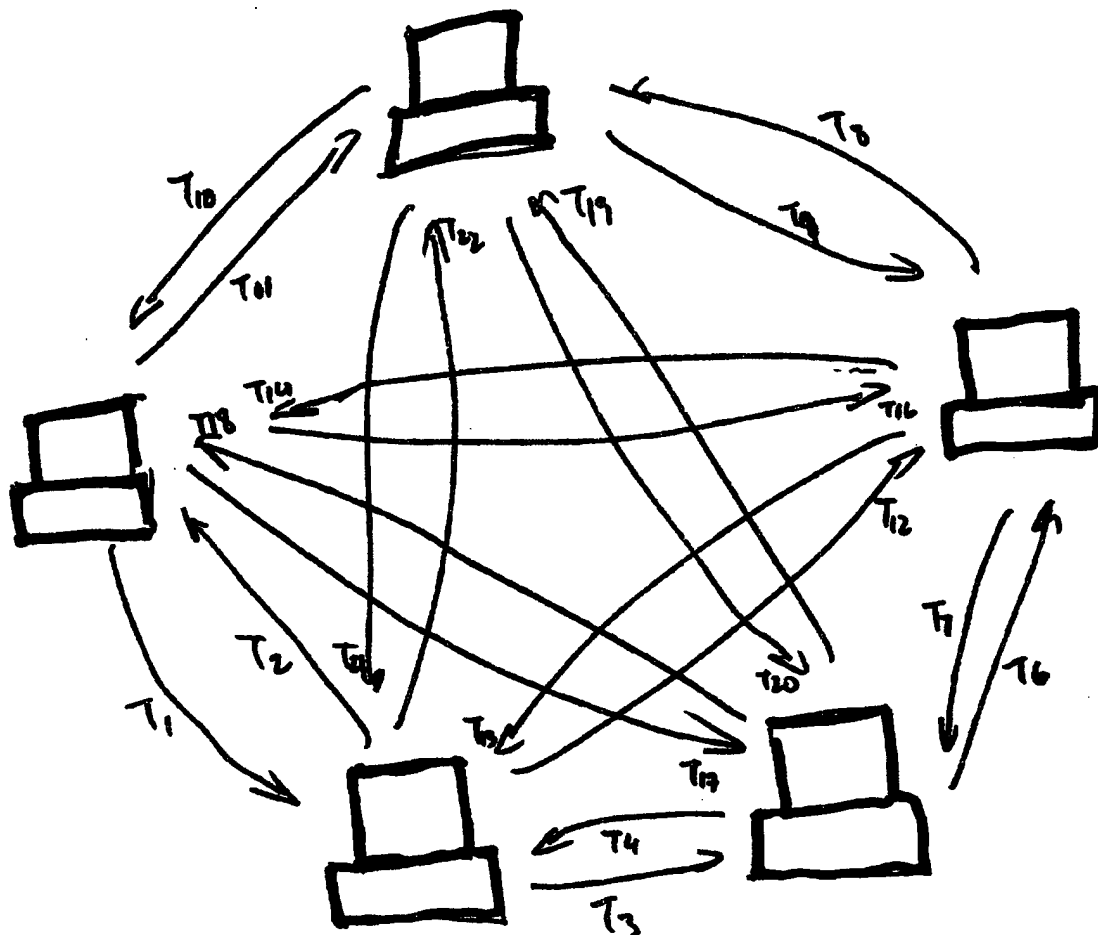


Fig 6.

Marks & Clerk

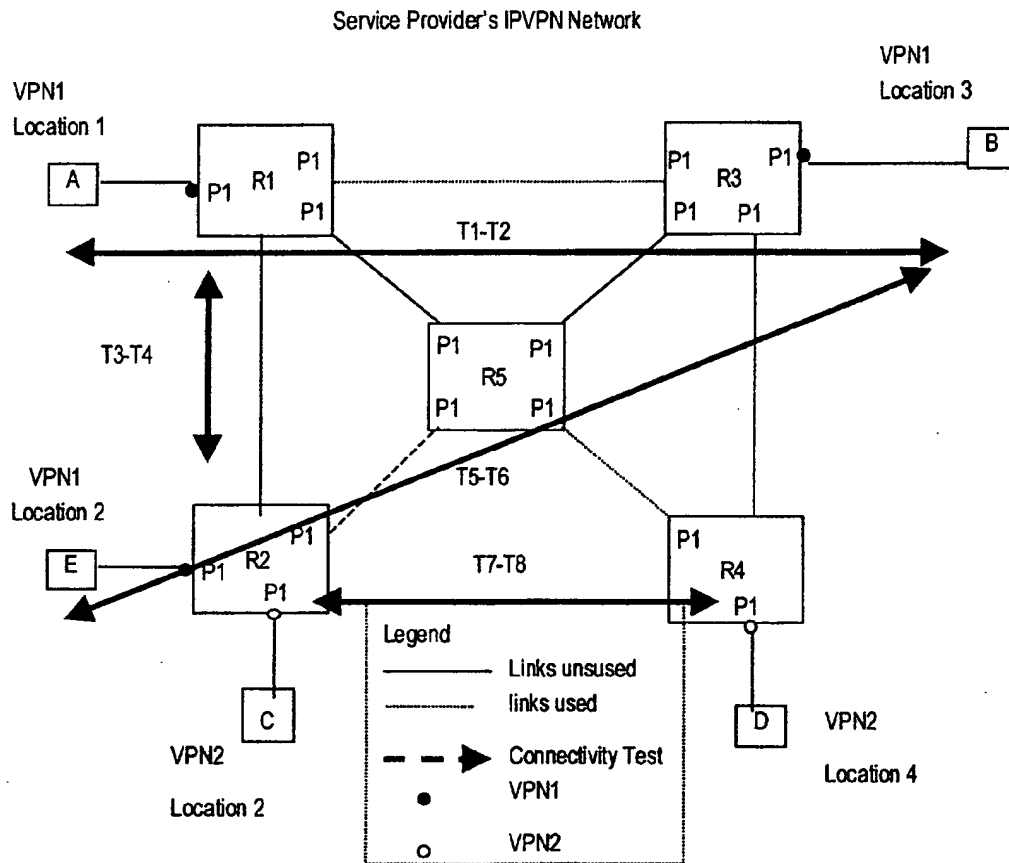


Figure 7 VPN Connectivity Test

Marks & Clerk

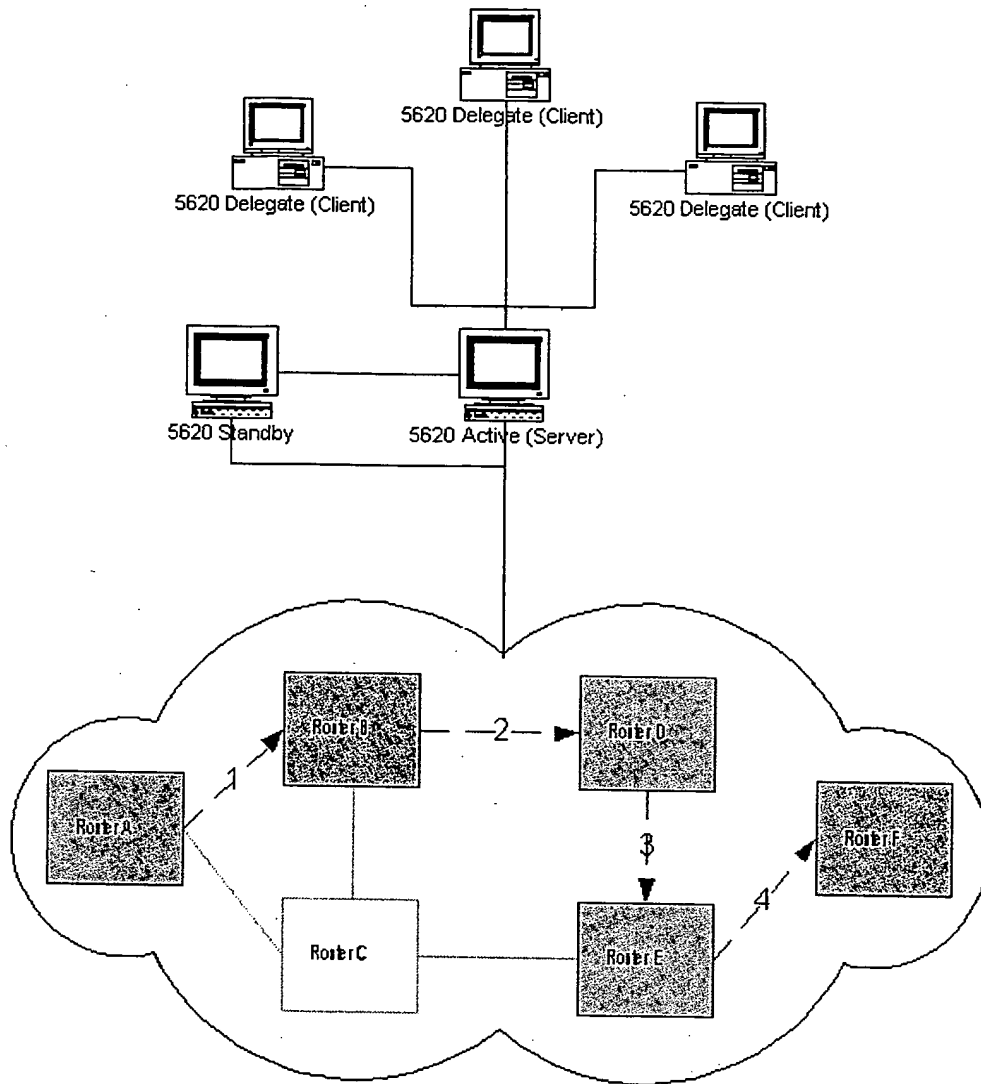


Figure 0-1: IP Maintenance and Diagnostics Operation System View

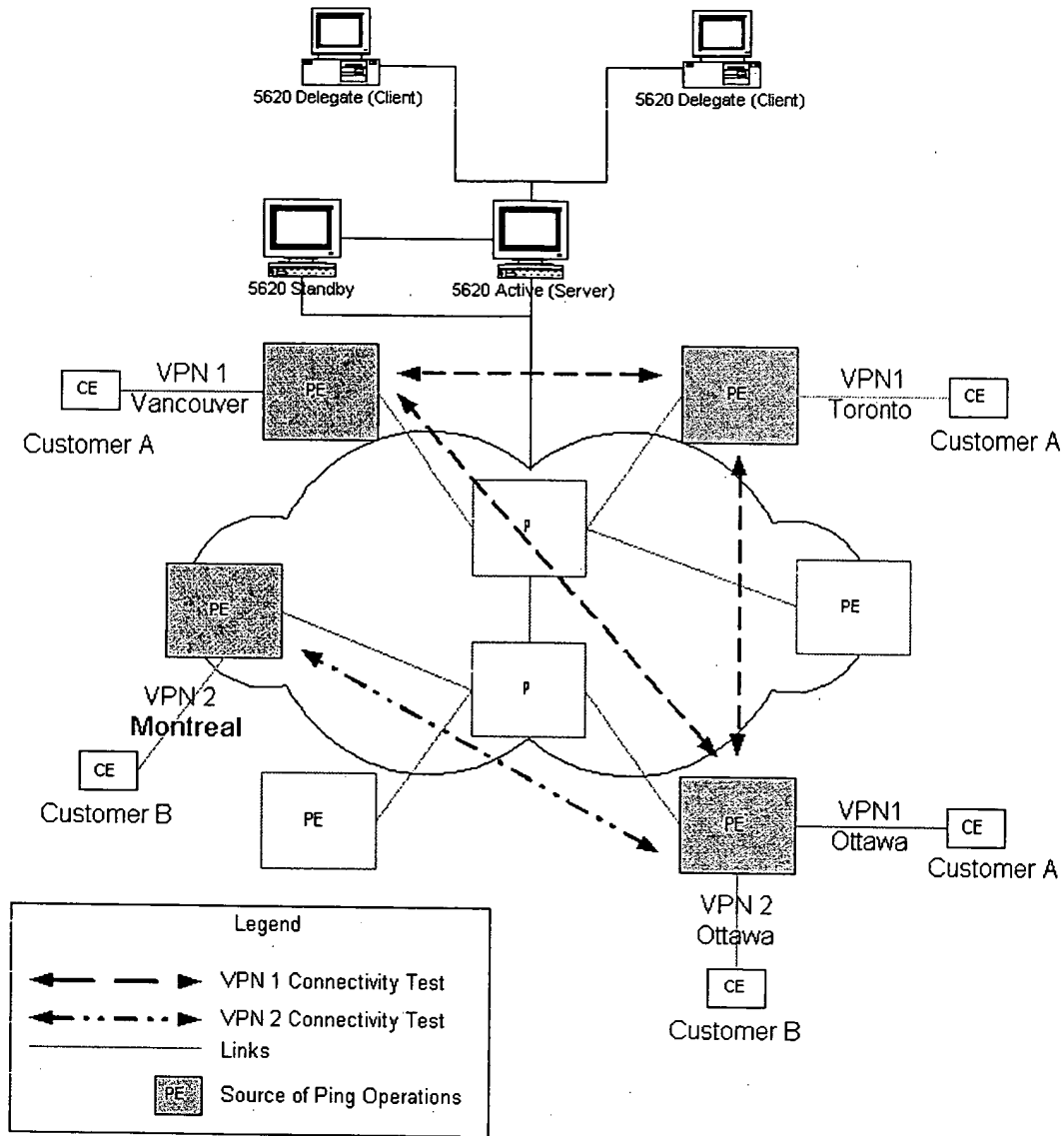


Figure 0-2: IP Maintenance and Diagnostics Scheduling System View

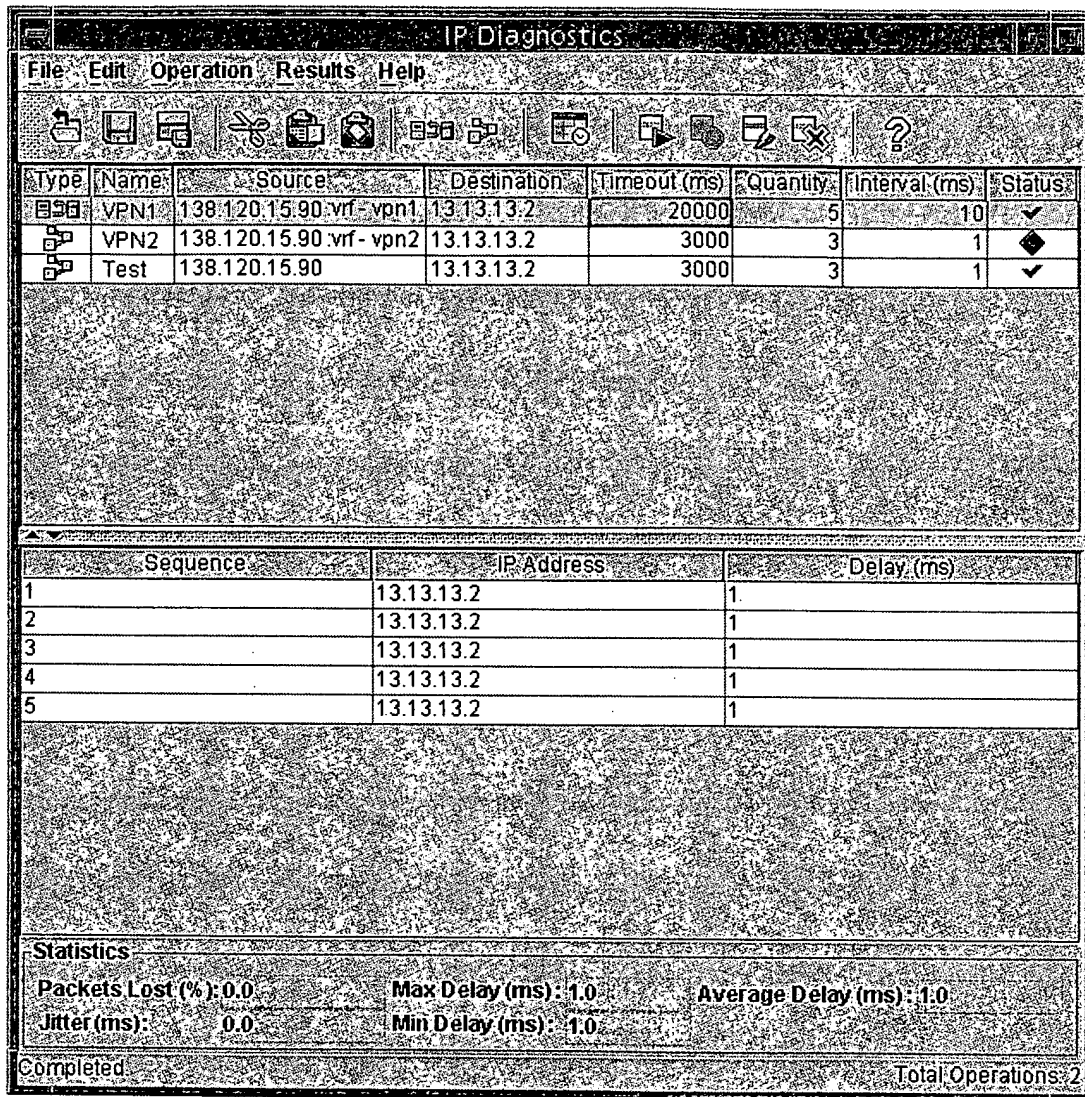


Figure 0-3: IP Maintenance and Diagnostics Operation Window

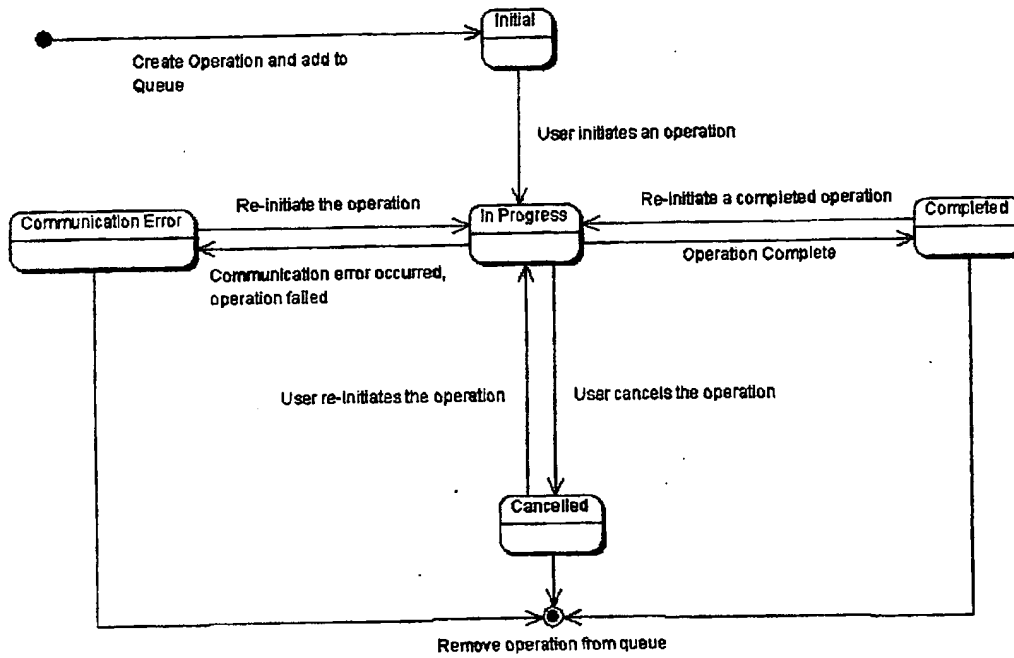


Figure 0-4: Operation Status State Diagram

Mark A. Clerk

| Statistics | | | |
|------------------|-----|--------------------|-----|
| Packets Lost (%) | 0.0 | Max Delay (ms) | 1.0 |
| Jitter (ms) | 0.0 | Average Delay (ms) | 1.0 |
| | | Min Delay (ms) | 1.0 |

Figure 0-6: Operation Statistics



Figure 0-7: Execution Error

IP Diagnostics Schedule

File Edit Operations Results Schedule Help

Enabled ☐ Schedule ☒ Start Time 10:10:00 End Time 10:12:00 Freq 1 Freq Period 1 minute(s) Alarm Status ☒ Status ☒

| Type | Access Name | Source | Destination | Alarm Status | Status |
|------|------------------|------------------------|-------------|-------------------------------------|-------------------------------------|
| B2D | Toronto - Ottawa | 138.120.15.90 vrf-vpn1 | 13.13.13.2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| B2D | Toronto - Van | 138.120.15.90 vrf-vpn1 | 13.13.13.3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| B2D | Ottawa - Toronto | 138.120.15.55 vrf-vpn1 | 13.13.13.2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| B2D | Ottawa - Van | 138.120.15.55 vrf-vpn1 | 13.13.13.1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| B2D | Van - Toronto | 138.120.15.20 vrf-vpn1 | 13.13.13.3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| B2D | Van - Ottawa | 138.120.15.20 vrf-vpn1 | 13.13.13.1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

| Time | Max Delay (ms) | Min Delay (ms) | Avg Delay (ms) | Jitter (ms) | Packet Loss % | Alarm Status | Status | Details |
|-------------------|----------------|----------------|----------------|-------------|---------------|-------------------------------------|-------------------------------------|---------|
| 02/10/03 10:10:00 | 120 | 10 | 59 | 50 | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 02/10/03 10:15:00 | 152 | 10 | 80 | 91 | 50 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 02/10/03 10:20:00 | 90 | 10 | 38 | 29 | 10 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 02/10/03 10:25:00 | 902 | 10 | 382 | 29 | 10 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 02/10/03 10:30:00 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |

Error: None

Completed Critical Alarm Raised Schedule Running Total Operations: 6

Figure 0-8: IP Maintenance and Diagnostics Scheduling Window

| Ping List | | | |
|---------------|------------|----------|------------------|
| Time | IP Address | Sequence | Delay (ms) |
| 02/20/03 4:00 | 12.12.12.1 | 1 | 7 |
| | 12.12.12.1 | 2 | 4 |
| | 12.12.12.1 | 3 | Node Unreachable |
| 02/20/03 4:10 | 12.12.12.1 | 1 | 7 |
| | 12.12.12.1 | 2 | 4 |
| | 12.12.12.1 | 3 | 4 |
| OK | | | |

Figure 0-9: Summary Ping List Window

Marks & Clerk

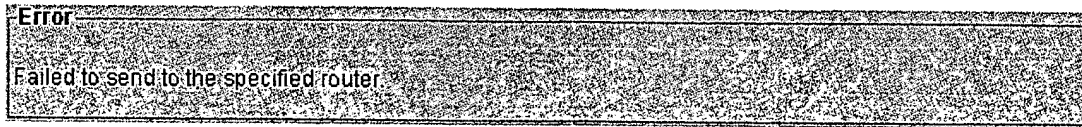


Figure 0-10: Execution Error

Schedule

General ☒ Schedule ☐ Thresholds

Schedule

Name: CustomerA - VPN1

Ping Setting

| | | | | | |
|------------------|----|-------------------|------------|------------------|----|
| Number of Pings: | 5 | Fill Pattern: | 0xABCDABCD | Packet Size: | 32 |
| Interval (sec): | 10 | Timeout per Ping: | 20000 | Type of Service: | 0 |

Add Cancel Help

Figure 0-11: Scheduling Configuration Window - General Tab

Morris & Clerk

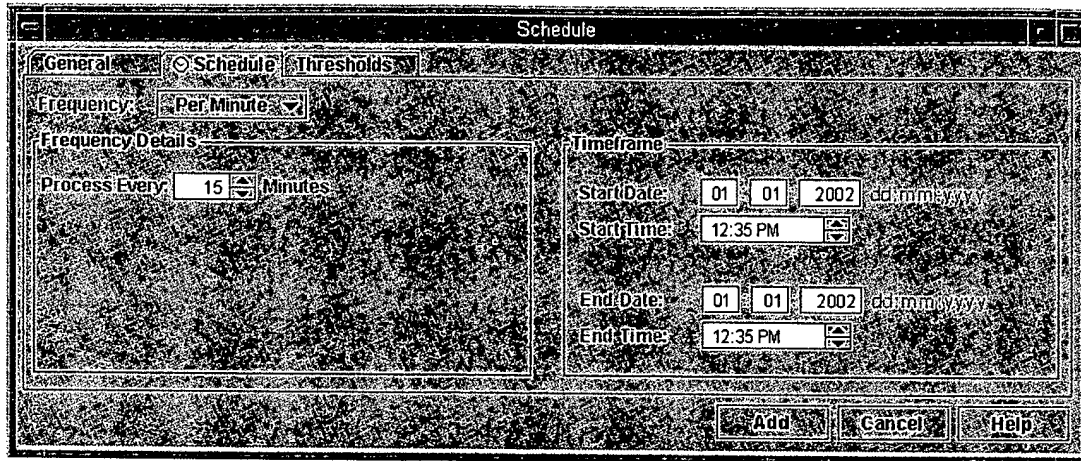


Figure 0-12: Scheduling Configuration Window - Schedule Tab

Morris & Clerk

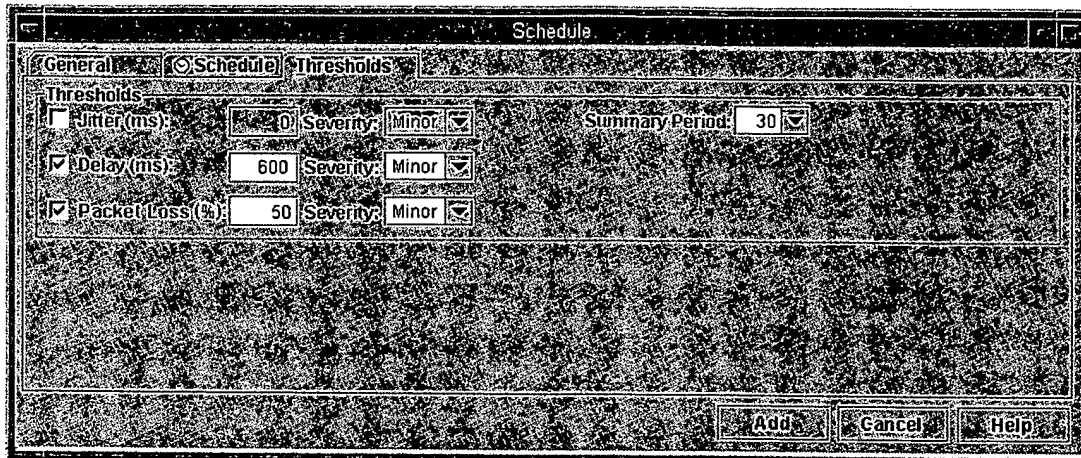


Figure 0-13: Scheduling Configuration Window - Threshold Tab

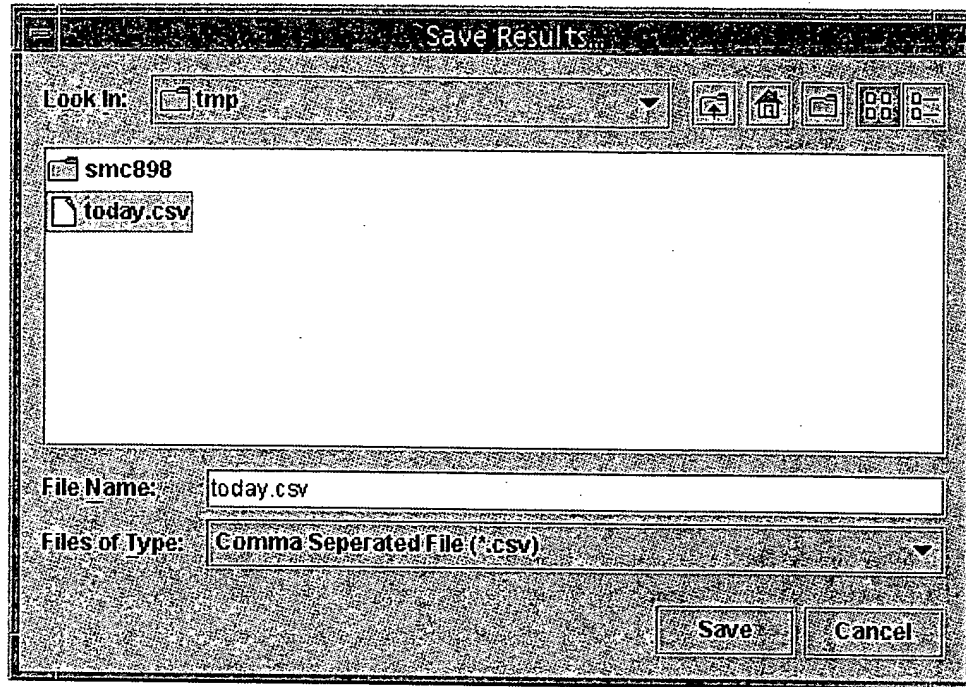


Figure 0-15: Save Results Dialog

Marks & Clerk

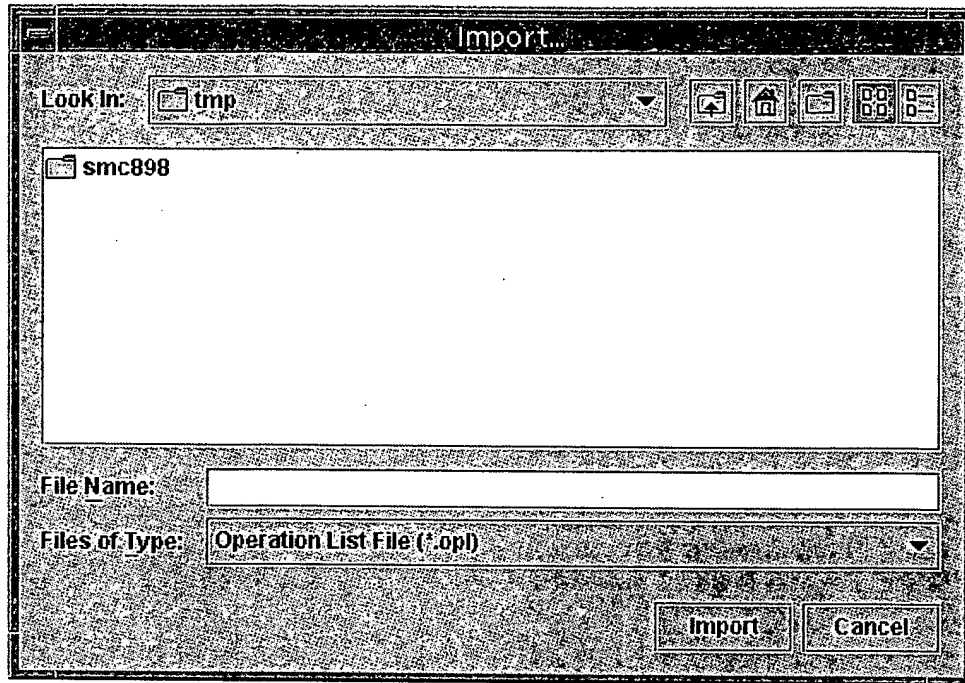


Figure 0-16: Open Operations an Operation List Dialog

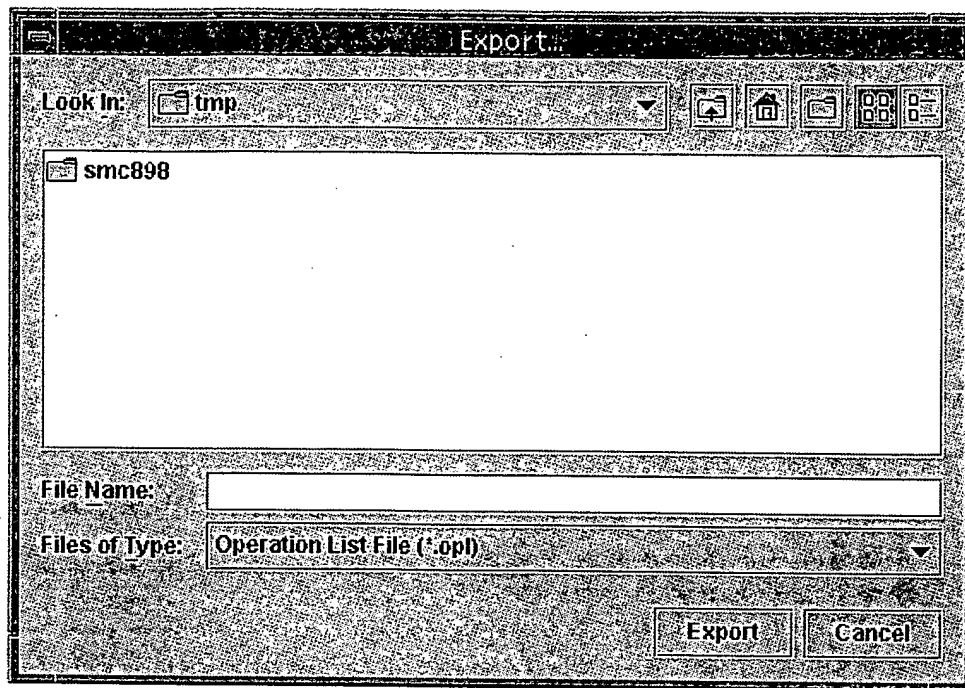


Figure 0-17: Save an Operation List Dialog

Martin & Clerk

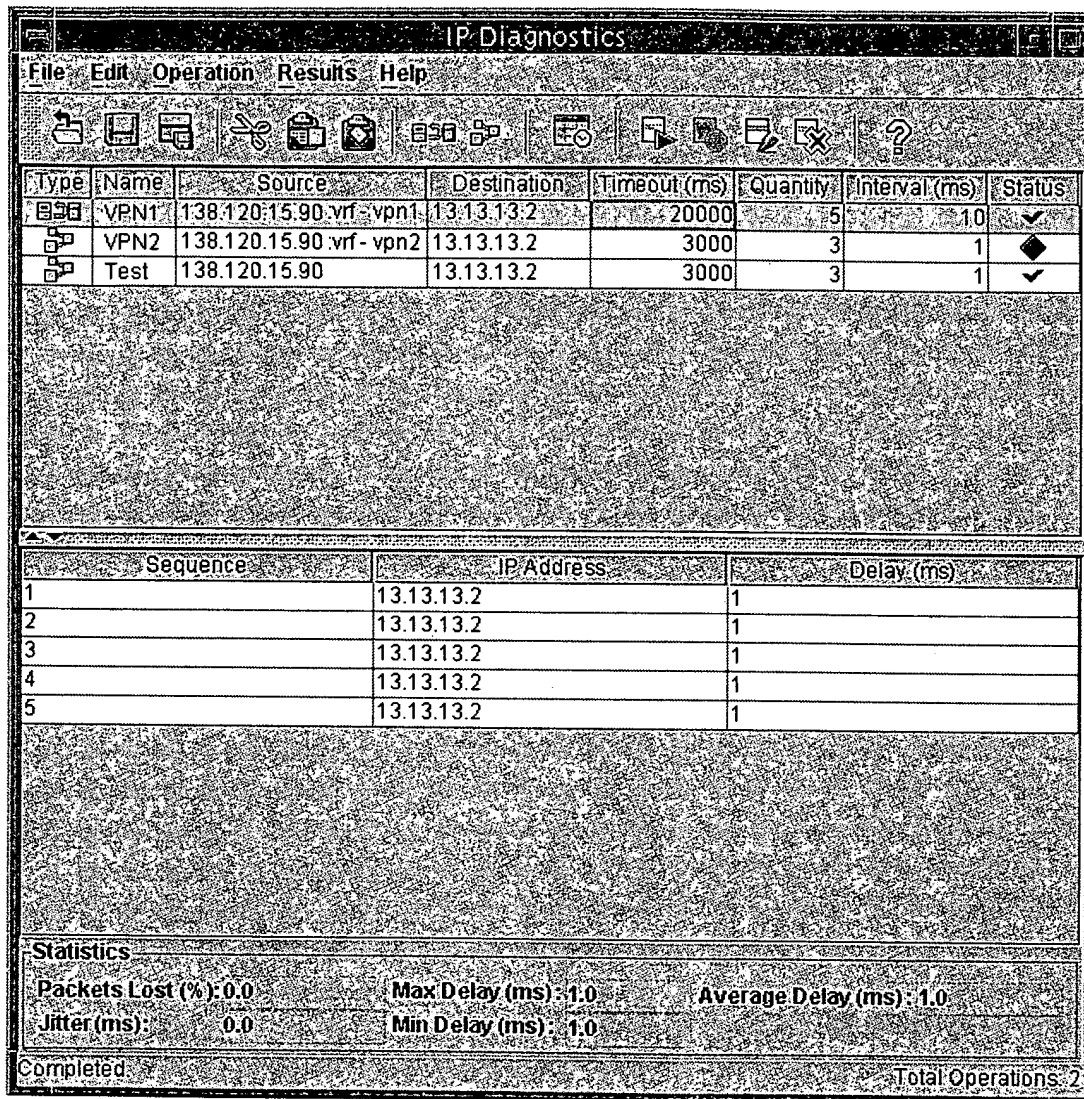


Figure 0-18: Ping Operation in the Operation List

Marks & Clerk

Ping

General
Name:

Source

☒ Router/Node:

☐ IP Address:

☐ LSP:

☐ Router Interface:

☐ VRF Name:

Destination

☒ Router/Node:

☐ IP Address/Router ID:

☐ LSP:

☐ Router Interface:

Ping Setting

| | | | | | |
|------------------|---------------------------------|-------------------|---|------------------|---------------------------------|
| Number of Pings: | <input type="text" value="5"/> | Fill Pattern: | <input type="text" value="0xABCDABCD"/> | Packet Size: | <input type="text" value="32"/> |
| Interval (sec): | <input type="text" value="10"/> | Timeout per Ping: | <input type="text" value="20000"/> | Type of Service: | <input type="text" value="0"/> |

Figure 0-19: Ping Window

Traceroute

General
Name:

Source

☒ Router Node:

☐ IP Address:

☐ LSP:

☐ Router Interface:

☐ VRF Name:

Destination

☐ Router Node:

☐ IP Address/Router ID:

☐ LSP:

☐ Router Interface:

Traceroute Setting

| | | | | | |
|--------------------|-----------------------------------|---------------|---|--------------|---------------------------------|
| Probes per Hop: | <input type="text" value="3"/> | Fill Pattern: | <input type="text" value="0xABCDABCD"/> | Packet Size: | <input type="text" value="32"/> |
| Interval (sec): | <input type="text" value="1"/> | UDP Port: | <input type="text" value="33434"/> | Maximum TTL: | <input type="text" value="30"/> |
| Timeout per Probe: | <input type="text" value="3000"/> | | | | |

Figure 0-21: Traceroute Window

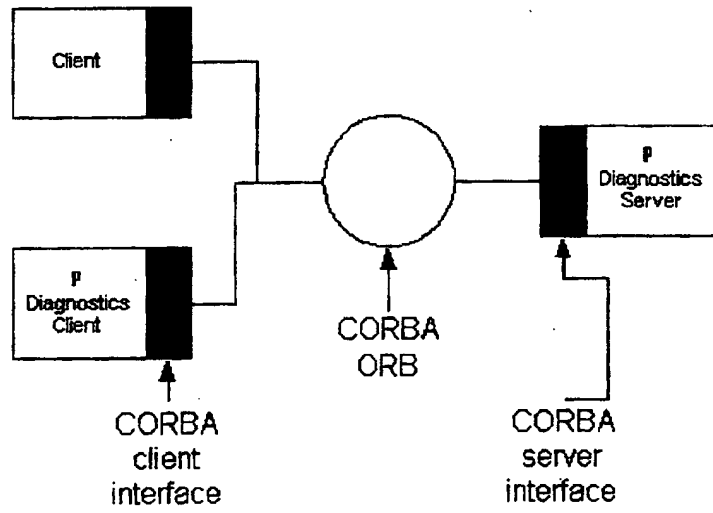


Figure 0-22: CORBA Interface

Martin & Clark

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.